



Guía del usuario

Amazon ECR



Versión de API 2015-09-21

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon ECR: Guía del usuario

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es Amazon ECR?	1
Componentes de Amazon ECR	1
Características de Amazon ECR	2
Primeros pasos con Amazon ECR	3
Precios de Amazon ECR	3
Cómo mover una imagen a lo largo de su ciclo de vida	4
Requisitos previos	4
Instale el AWS CLI	4
Instalar Docker	4
Paso 1: creación de una imagen de Docker	6
Paso 2: autenticar en su registro predeterminado	8
Paso 3: crear un repositorio	9
Paso 4: Insertar una imagen en Amazon ECR	9
Paso 5: Extraer una imagen de Amazon ECR	11
Paso 6: eliminar una imagen	11
Paso 7: eliminar un repositorio	12
Optimización del rendimiento	13
Registro privado	15
Conceptos sobre el registro	15
Autenticación del registro	15
Uso del ayudante de credenciales de Amazon ECR	16
Uso de un token de autorización	16
Uso de la autenticación de la API HTTP	17
Opciones del registro	18
Permisos de registro	19
Ejemplos de políticas de registro	20
Otorgar permisos para la replicación entre cuentas	22
Otorgar permisos para extraer la memoria caché	24
Repositorios privados	26
Conceptos sobre los repositorios	26
Crear un repositorio para almacenar imágenes	27
Sigüientes pasos	28
Visualización de detalles de repositorios	28
Eliminación de un repositorio	30

Políticas de repositorios	30
Políticas de repositorios frente a políticas de IAM	31
Ejemplos de políticas de repositorio	32
Configuración de una instrucción de política de repositorio	38
Etiquetado de un repositorio	40
Conceptos básicos de etiquetas	40
Etiquetado de los recursos para facturación	40
Agregar etiquetas.	41
Eliminación de etiquetas	42
Imágenes privadas	44
Insertar una imagen	44
Permisos de IAM necesarios	45
Inserción de una imagen de Docker	46
Empujar una imagen multiarquitectura	48
Inserción de un gráfico de Helm	50
Firma de una imagen	52
Consideraciones	52
Requisitos previos	53
Configurar la autenticación para el cliente Notary	53
Firma de una imagen	53
Sigüientes pasos	55
Eliminación de una firma	55
Visualización de los detalles de imagen	56
Extraer una imagen	56
Extracción de la imagen del contenedor de Amazon Linux	58
Eliminar una imagen	59
Volver a etiquetar una imagen	61
Impedir que las etiquetas de imagen se sobrescriban	64
Configurar la mutabilidad de las etiquetas de imagen (AWS Management Console)	64
Establecer la mutabilidad de la etiqueta de imagen (AWS CLI)	65
Formatos del manifiesto de imágenes de contenedor	66
Conversión del manifiesto de imagen de Amazon ECR	66
Uso de imágenes de Amazon ECR con Amazon ECS	67
Permisos de IAM necesarios	67
Especificación de una imagen de Amazon ECR en una definición de tarea	69
Uso de imágenes de Amazon ECR con Amazon EKS	70

Permisos de IAM necesarios	70
Instalación de un gráfico de Helm en un clúster de Amazon EKS	71
Escanee las imágenes en busca de vulnerabilidades	74
Filtros para repositorios	75
Filtra los caracteres comodín	75
Escaneo mejorado	76
Consideraciones del escaneo mejorado	76
Permisos de IAM necesarios	78
Configuración del escaneo mejorado	79
Cambio de la duración del análisis mejorado	81
EventBridge eventos	81
Recuperando los resultados	87
Escaneo básico	88
Soporte regional para mejorar el escaneo básico	89
Compatibilidad con el sistema operativo para el escaneo básico y un escaneo básico mejorado	90
Configuración del escaneo básico mejorado	91
Configuración del escaneo básico	92
Escaneo manual de una imagen	93
Recuperando los resultados	94
Solución de problemas de digitalización de imágenes	96
Descripción del estado de análisis SCAN_ELIGIBILITY_EXPIRED	97
Sincronice un registro anterior	98
Plantillas de creación de repositorios	98
Consideraciones sobre el uso de las reglas de extracción de caché	99
Permisos de IAM necesarios	101
Uso de permisos de registro	102
Sigüientes pasos	103
Creación de una regla de caché de extracción	104
Requisitos previos	104
Usando la AWS Management Console	104
Utilización del AWS CLI	111
Sigüientes pasos	114
Plantillas de creación de repositorios	114
Funcionamiento	115
Permisos de IAM necesarios	118

Crear una plantilla de creación de repositorios	118
Eliminar una plantilla de creación de repositorios	121
Validación de la regla de extracción de caché	121
Extracción de una imagen con una regla de caché de extracción	122
Almacenar en secreto las credenciales del repositorio principal	124
Solución de problemas con la caché de extracción	132
Replica imágenes	134
Consideraciones sobre la replicación de imágenes privadas	134
Ejemplos de replicación	136
Ejemplo: Configurar la replicación entre regiones en una única región de destino	136
Ejemplo: Configurar la replicación entre regiones mediante un filtro de repositorio	136
Ejemplo: Configurar la replicación entre regiones en varias regiones de destino	137
Ejemplo: Configurar la replicación entre cuentas	137
Ejemplo: Especificar varias reglas en una configuración	138
Configuración de la replicación	139
Automatice la limpieza de imágenes	142
Funcionamiento de las políticas de ciclo de vida	142
Reglas de evaluación de políticas de ciclo de vida	143
Creación de una vista previa de política de ciclo de vida	144
Crear una política de ciclo de vida	146
Requisito previo	147
Ejemplos de políticas de ciclo de vida	149
Plantilla de política de ciclo de vida	149
Filtrar por antigüedad de las imágenes	149
Filtrar por el número de imágenes	150
Filtrar por varias reglas	151
Filtrar por varias etiquetas en una sola regla	153
Filtrar por todas las imágenes	156
Propiedades de la política de ciclo de	158
Prioridad de las reglas	159
Descripción	159
Estado de etiqueta	159
Lista de patrones de etiquetas	160
Lista de prefijos de etiqueta	160
Tipo de recuento	161
Unidad de recuento	161

Cantidad	161
Acción	162
Seguridad	163
Identity and Access Management	164
Público	164
Autenticación con identidades	165
Administración de acceso mediante políticas	168
Cómo funciona Amazon Elastic Container Registry con IAM	171
Ejemplos de políticas basadas en identidades	176
Uso del control de acceso basado en etiquetas	181
AWS políticas gestionadas para Amazon ECR	183
Uso de roles vinculados a servicios	192
Resolución de problemas	198
Protección de datos	200
Cifrado en reposo	201
Validación de conformidad	208
Seguridad de infraestructuras	210
Puntos de conexión de VPC de interfaz (AWS PrivateLink)	211
Prevención de la sustitución confusa entre servicios	220
Supervisión	223
Visualización de Service Quotas y configuración de alarmas	224
Métricas de uso	225
Informes de uso de	227
Métricas de repositorios	227
Habilitar CloudWatch las métricas	227
Métricas y dimensiones disponibles	228
Visualización de las métricas con CloudWatch	228
Eventos y EventBridge	229
Eventos de ejemplo de Amazon ECR	229
Registro de acciones de AWS CloudTrail con	233
Información de Amazon ECR en CloudTrail	234
Descripción de las entradas de archivos de registros de Amazon ECR	235
Trabajar con SDK AWS	247
Ejemplos de código	249
Acciones	249
DescribeRepositories	249

ListImages	251
Cuotas de servicio	254
Administración de las cuotas de servicio de Amazon ECR en la AWS Management Console ...	259
Creación de una alarma de CloudWatch para monitorear las métricas de uso de las API	260
Resolución de problemas	262
Solución de problemas de Docker	262
Los registros de Docker no contienen los mensajes de error esperados	262
Error «Filesystem Verification Failed» (Fallo al verificar el sistema de archivos) o «404: Image Not Found» (Imagen no encontrada) al extraer una imagen de un repositorio de Amazon ECR	263
Error «Filesystem Layer Verification Failed» (Fallo al verificar la capa del sistema de archivos) al extraer imágenes de Amazon ECR	264
Errores HTTP 403 o error «no basic auth credentials» (no hay credenciales de autenticación básica) al insertar contenido en un repositorio	264
Solución de problemas de los mensajes de error de Amazon ECR	265
HTTP 429: demasiadas solicitudes o ThrottleException	265
HTTP 403: "User [arn] is not authorized to perform [operación]"	266
Error HTTP 404: «Repository Does Not Exist» (El repositorio no existe)	266
Error: No se puede realizar un inicio de sesión interactivo desde un dispositivo que no sea TTY	267
Historial de documentos	268
.....	cclxxv

¿Qué es Amazon Elastic Container Registry?

Amazon Elastic Container Registry (Amazon ECR) es AWS un servicio gestionado de registro de imágenes de contenedores seguro, escalable y fiable. Amazon ECR admite repositorios privados con permisos basados en recursos mediante IAM. AWS De este modo, los usuarios especificados o las instancias de Amazon EC2 pueden acceder a sus repositorios e imágenes de contenedor. Puede utilizar la CLI preferida para insertar, extraer y administrar imágenes de Docker, imágenes de Open Container Initiative (OCI) y artefactos compatibles con OCI.

Note

Amazon ECR también admite repositorios de imágenes de contenedor públicos. Para obtener más información, consulte [¿Qué es Amazon ECR Public?](#) en la Guía del usuario de Amazon ECR Public.

El equipo de servicios de AWS contenedores mantiene una hoja de ruta pública. GitHub Contiene información sobre en qué están trabajando los equipos y permite a todos AWS los clientes dar su opinión directamente. Para obtener más información, consulte [Guía de contenedores de AWS](#).

Componentes de Amazon ECR

Amazon ECR contiene los siguientes componentes:

Registro

Se proporciona un registro privado de Amazon ECR para cada AWS cuenta; puede crear uno o más repositorios en su registro y almacenar en ellos imágenes de Docker, imágenes de Open Container Initiative (OCI) y artefactos compatibles con OCI. Para obtener más información, consulte [Registro privado de Amazon ECR](#).

Token de autorización

Su cliente debe autenticarse en un registro privado de Amazon ECR como usuario de AWS antes de poder enviar y extraer imágenes. Para obtener más información, consulte [Autenticación de registro privado en Amazon ECR](#).

Repositorio

Un repositorio de Amazon ECR contiene las imágenes de Docker, las imágenes de Open Container Initiative (OCI) y artefactos compatibles con OCI. Para obtener más información, consulte [Repositorios privados de Amazon ECR](#).

Política sobre repositorios

Puede controlar el acceso a los repositorios y al contenido que portan mediante políticas. Para obtener más información, consulte [Políticas de repositorios privados en Amazon ECR](#).

Imagen

Puede insertar y extraer imágenes de contenedor en los repositorios y utilizarlas localmente en su sistema de desarrollo o en definiciones de tareas de Amazon ECS y especificaciones del pod de Amazon EKS. Para obtener más información, consulte [Uso de imágenes de Amazon ECR con Amazon ECS](#) y [Uso de imágenes de Amazon ECR con Amazon EKS](#).

Características de Amazon ECR

Amazon ECR ofrece las siguientes características:

- Las políticas de ciclo de vida ayudan a administrar el ciclo de vida de las imágenes en sus repositorios. Debe definir reglas que den como resultado la limpieza de imágenes no utilizadas. Puede probar reglas antes de aplicarlas al repositorio. Para obtener más información, consulte [Automatice la limpieza de imágenes mediante políticas de ciclo de vida en Amazon ECR](#).
- El escaneo de imágenes permite identificar vulnerabilidades de software en las imágenes de contenedor. Los repositorios se pueden configurar para escanear al insertar. Esto garantiza que cada nueva imagen insertada al repositorio se escanee. A continuación, puede recuperar los resultados del escaneo de la imagen. Para obtener más información, consulte [Escanee imágenes en busca de vulnerabilidades de software en Amazon ECR](#).
- La replicación entre regiones y entre cuentas hace que sea más fácil tener las imágenes donde las necesite. Se configura como un parámetro del Registro y se aplica por región. Para obtener más información, consulte [Configuración de registro privado en Amazon ECR](#).
- Las reglas de caché de extracción proporcionan una manera de almacenar en caché los repositorios en un registro ascendente en su registro privado de Amazon ECR. Al utilizar una regla de caché de extracción, Amazon ECR se comunicará periódicamente con el registro ascendente para garantizar que la imagen almacenada en caché en su registro privado de Amazon ECR esté

actualizada. Para obtener más información, consulte [Sincronice un registro anterior con un registro privado de Amazon ECR](#).

Primeros pasos con Amazon ECR

Si utiliza Amazon Elastic Container Service (Amazon ECS) o Amazon Elastic Kubernetes Service (Amazon EKS), tenga en cuenta que la configuración de estos dos servicios es similar a la configuración de Amazon ECR, ya que Amazon ECR es una extensión de ambos servicios.

Cuando utilice Amazon ECR, utilice una versión de AWS CLI que sea compatible AWS Command Line Interface con las funciones más recientes de Amazon ECR. Si no ve compatibilidad con una función de Amazon ECR en AWS CLI, actualice a la última versión de AWS CLI. Para obtener información sobre la instalación de la última versión de AWS CLI, consulte [Instalar o actualizar a la última versión de AWS CLI en la](#) Guía del AWS Command Line Interface usuario.

Para obtener información sobre cómo insertar una imagen de contenedor en un repositorio privado de Amazon ECR mediante AWS CLI y Docker, consulte. [Cómo mover una imagen a lo largo de su ciclo de vida en Amazon ECR](#)

Precios de Amazon ECR

Con Amazon ECR, solo pagará por la cantidad de datos que almacene en sus repositorios, y por la transferencia de datos de sus inserciones y extracciones de imágenes. Para obtener más información, consulte los [Precios de Amazon ECR](#).

Cómo mover una imagen a lo largo de su ciclo de vida en Amazon ECR

Si utiliza Amazon ECR por primera vez, siga los siguientes pasos con la CLI de Docker y AWS CLI para crear una imagen de muestra, autenticarse en el registro predeterminado y crear un repositorio privado. A continuación, inserte una imagen en el repositorio privado y extráigala. Cuando termine con la imagen de muestra, borra la imagen de muestra y el repositorio.

Para usar el AWS Management Console en lugar del AWS CLI, consulte [the section called “Crear un repositorio para almacenar imágenes”](#).

[Para obtener más información sobre las demás herramientas disponibles para administrar AWS los recursos, incluidos los distintos AWS SDK, los kits de herramientas del IDE y las herramientas de línea de PowerShell comandos de Windows, consulte <http://aws.amazon.com/tools/>.](#)

Requisitos previos

Si no dispone de la última versión AWS CLI ni de Docker instalado y listo para usarse, siga estos pasos para instalar ambas herramientas.

Instale el AWS CLI

Para usarlo AWS CLI con Amazon ECR, instale la AWS CLI versión más reciente. Para obtener información, consulte [Instalar la AWS Command Line Interface](#) en la Guía del usuario de AWS Command Line Interface .

Instalar Docker

Docker está disponible en muchos sistemas operativos diferentes, incluidas las distribuciones de Linux más modernas, como Ubuntu, e incluso en macOS y Windows. Para obtener más información sobre cómo instalar Docker en su sistema operativo concreto, consulte la [guía de instalación de Docker](#).

No necesita un sistema de desarrollo local para usar Docker. Si ya utiliza Amazon EC2, puede lanzar una instancia de Amazon Linux 2023 e instalar Docker para empezar.

Si ya tiene Docker instalado, pase a [Paso 1: creación de una imagen de Docker](#).

Instalación de Docker en una instancia de Amazon EC2 mediante una AMI de Amazon Linux 2023

1. Lance una instancia con la AMI de Amazon Linux 2023. Para obtener más información, consulte [Lanzamiento de una instancia](#) en la Guía del usuario de Amazon EC2.
2. Conecte con la instancia . Para obtener más información, consulte [Conectarse a su instancia de Linux](#) en la Guía del usuario de Amazon EC2.
3. Actualice la caché de paquetes y los paquetes instalados en la instancia.

```
sudo yum update -y
```

4. Instale el paquete de Community Edition de Docker más reciente.

```
sudo yum install docker
```

5. Abra el servicio de Docker.

```
sudo service docker start
```

6. Agregue el `ec2-user` al grupo `docker` para que pueda ejecutar comandos de Docker sin usar `sudo`.

```
sudo usermod -a -G docker ec2-user
```

7. Cierre sesión y vuelva a iniciarla para actualizar los nuevos permisos de grupo de `docker`. Para ello, cierre la ventana de su terminal de SSH actual y vuelva a conectarse a la instancia en una ventana nueva. De esta forma, la nueva sesión de SSH tendrá los permisos de grupo de `docker` adecuados.
8. Compruebe que el `ec2-user` puede ejecutar comandos de Docker sin `sudo`.

```
docker info
```

Note

En algunos casos, es posible que tenga que reiniciar su instancia para que el `ec2-user` tenga los permisos necesarios para acceder al daemon de Docker. Intente reiniciar su instancia si ve el siguiente error:

Cannot connect to the Docker daemon. Is the docker daemon running on this host?

Paso 1: creación de una imagen de Docker

En este paso, va a crear una imagen de Docker de una aplicación web simple y la va a probar en su sistema local o en la instancia de Amazon EC2.

Creación de una imagen Docker de una aplicación web simple

1. Cree un archivo denominado `Dockerfile`. Un `Dockerfile` es un manifiesto que describe la imagen base para su imagen Docker y qué desea instalar y que se ejecute en ella. Para obtener más información acerca de los archivos Docker, consulte [Docker Reference](#).

```
touch Dockerfile
```

2. Edite el `Dockerfile` que acaba de crear y agregue el siguiente contenido.

```
FROM public.ecr.aws/amazonlinux/amazonlinux:latest

# Install dependencies
RUN yum update -y && \
    yum install -y httpd

# Install apache and write hello world message
RUN echo 'Hello World!' > /var/www/html/index.html


# Configure apache
RUN echo 'mkdir -p /var/run/httpd' >> /root/run_apache.sh && \
    echo 'mkdir -p /var/lock/httpd' >> /root/run_apache.sh && \
    echo '/usr/sbin/httpd -D FOREGROUND' >> /root/run_apache.sh && \
    chmod 755 /root/run_apache.sh

EXPOSE 80

CMD /root/run_apache.sh
```

Este Dockerfile utiliza la imagen pública de Amazon Linux 2 alojada en Amazon ECR Public. Las instrucciones RUN actualizan la caché del paquete, instalan algunos paquetes de software para el servidor web y, a continuación, escriben el contenido “Hello World!” en la raíz de documentos del servidor web. El folleto EXPOSE expone el puerto 80 en el contenedor y las instrucciones CMD inician el servidor web.

3. Cree la imagen Docker desde el Dockerfile.

 Note

Algunas versiones de Docker pueden requerir la ruta completa a su Dockerfile en el siguiente comando en lugar de la ruta relativa que se muestra a continuación.

```
docker build -t hello-world .
```

4. Incluya la imagen de su contenedor.

```
docker images --filter reference=hello-world
```

Salida:

REPOSITORY	TAG	IMAGE ID	CREATED
hello-world	latest	e9ffedc8c286	4 minutes ago
SIZE			
194MB			

5. Ejecute la nueva imagen. La opción `-p 80:80` asigna el puerto 80 expuesto en el contenedor al puerto 80 del sistema de host. Para obtener más información acerca de `docker run`, diríjase a la [referencia de ejecución de Docker](#).

```
docker run -t -i -p 80:80 hello-world
```

Note

La salida desde el servidor web Apache se muestra en la ventana de la terminal. Puede hacer caso omiso del mensaje "Could not reliably determine the fully qualified domain name"

- Abra un navegador y encuentre el servidor que está ejecutando Docker y alojando su contenedor.
 - Si utiliza una instancia de EC2, este es el valor DNS público para el servidor, que es la misma dirección que utiliza para conectarse a la instancia con SSH. Asegúrese de que el grupo de seguridad para la instancia permite el tráfico entrante en el puerto 80.
 - Si ejecuta Docker de forma local, dirija el navegador a <http://localhost/>.
 - Si lo utiliza docker-machine en un ordenador Windows o Mac, busque la dirección IP de la VirtualBox máquina virtual que aloja Docker con el `docker-machine ip` comando y sustituya el nombre de la *máquina docker por el nombre de la máquina* docker que está utilizando.

```
docker-machine ip machine-name
```

Debería ver una página web que diga "Hello, World!" statement.

- Detenga el contenedor de Docker escribiendo Ctrl + c.

Paso 2: autenticar en su registro predeterminado

Una vez que haya instalado y configurado AWS CLI, autentique la CLI de Docker en su registro predeterminado. De este modo, el comando docker puede extraer e insertar imágenes con Amazon ECR. AWS CLI Proporciona un `get-login-password` comando para simplificar el proceso de autenticación.

Para autenticar Docker en un registro de Amazon ECR con `get-login-password`, ejecute el comando `aws ecr get-login-password` Al pasar el token de autenticación al comando `docker login`, utilice el valor AWS para el nombre de usuario y especifique el URI del registro de Amazon ECR en el que desea autenticarse. Si se autentica en varios registros, deberá repetir el comando con cada registro.

⚠ Important

Si recibe un error, instale o actualice a la versión más reciente de la AWS CLI. Para obtener más información, consulte [Installing the AWS Command Line Interface](#) en la Guía del usuario de AWS Command Line Interface .

- [get-login-password](#) (AWS CLI)

```
aws ecr get-login-password --region region | docker login --username AWS --password-stdin aws_account_id.dkr.ecr.region.amazonaws.com
```

- [Get-ECR \(\) LoginCommand](#) AWS Tools for Windows PowerShell

```
(Get-ECRLoginCommand).Password | docker login --username AWS --password-stdin aws_account_id.dkr.ecr.region.amazonaws.com
```

Paso 3: crear un repositorio

Ahora que ya tiene una imagen para insertar en Amazon ECR, debe crear un repositorio para almacenarla. En este ejemplo, va a crear un repositorio llamado `hello-repository` en el que insertará después la imagen `hello-world:latest`. Para crearlo, ejecute este comando:

```
aws ecr create-repository \  
  --repository-name hello-repository \  
  --region region
```

Paso 4: Insertar una imagen en Amazon ECR

Ahora puede insertar la imagen en el repositorio de Amazon ECR que ha creado en la sección anterior. Utilice la docker CLI para enviar imágenes una vez que se cumplan los siguientes requisitos previos:

- La versión mínima de docker está instalada: 1.7.
- El token de autorización de Amazon ECR se configuró con `docker login`.
- Debe existir el repositorio de Amazon ECR y el usuario debe disponer de acceso para insertar imágenes en él.

Si se cumplen estos requisitos previos, podrá insertar la imagen en el repositorio recién creado del registro predeterminado de su cuenta.

Etiquetado e inserción de una imagen en Amazon ECR

1. Muestre las imágenes que ha almacenado localmente para identificar la que desea etiquetar e insertar.

```
docker images
```

Salida:

REPOSITORY	TAG	IMAGE ID	CREATED
hello-world	latest	e9ffedc8c286	4 minutes ago
241MB			

2. Etiquete la imagen que desea insertar en el repositorio.

```
docker tag hello-world:latest aws_account_id.dkr.ecr.region.amazonaws.com/hello-repository
```

3. Inserte la imagen.

```
docker push aws_account_id.dkr.ecr.region.amazonaws.com/hello-repository
```

Salida:

```
The push refers to a repository [aws_account_id.dkr.ecr.region.amazonaws.com/hello-repository] (len: 1)
e9ae3c220b23: Pushed
a6785352b25c: Pushed
0998bf8fb9e9: Pushed
0a85502c06c9: Pushed
latest: digest: sha256:215d7e4121b30157d8839e81c4e0912606fca105775bb0636EXAMPLE
size: 6774
```

Paso 5: Extraer una imagen de Amazon ECR

Una vez que la imagen se haya enviado a su repositorio de Amazon ECR, podrá extraerla de otras ubicaciones. Utilice la docker CLI para extraer imágenes una vez que se cumplan los siguientes requisitos previos:

- La versión mínima de docker está instalada: 1.7.
- El token de autorización de Amazon ECR se configuró con `docker login`.
- Debe existir el repositorio de Amazon ECR y el usuario debe tener acceso para extraer imágenes de él.

Si se cumplen estos requisitos previos, podrá extraer la imagen. Para extraer la imagen de ejemplo de Amazon ECR, ejecute este comando:

```
docker pull aws_account_id.dkr.ecr.region.amazonaws.com/hello-repository:latest
```

Salida:

```
latest: Pulling from hello-repository
0a85502c06c9: Pull complete
0998bf8fb9e9: Pull complete
a6785352b25c: Pull complete
e9ae3c220b23: Pull complete
Digest: sha256:215d7e4121b30157d8839e81c4e0912606fca105775bb0636EXAMPLE
Status: Downloaded newer image for aws_account_id.dkr.region.amazonaws.com/hello-repository:latest
```

Paso 6: eliminar una imagen

Si ya no necesita una imagen en uno de sus repositorios, puede eliminarla. Para eliminar una imagen, especifica el repositorio en el que se encuentra y un `imageDigest` valor `imageTag` o para la imagen. En el siguiente ejemplo, se elimina una imagen del `hello-repository` repositorio con la etiqueta `latest` de imagen. Para eliminar la imagen de ejemplo del repositorio, ejecuta el siguiente comando:

```
aws ecr batch-delete-image \  
  --repository-name hello-repository \  
  --image-ids imageDigest
```

```
--image-ids imageTag=latest \  
--region region
```

Paso 7: eliminar un repositorio

Si ya no necesitas un repositorio completo de imágenes, puedes eliminarlo. En el siguiente ejemplo, se utiliza la `--force` marca para eliminar un repositorio que contiene imágenes. Para eliminar un repositorio que contiene imágenes (y todas las imágenes con él), ejecute este comando:

```
aws ecr delete-repository \  
  --repository-name hello-repository \  
  --force \  
  --region region
```

Optimización del rendimiento en Amazon ECR

Puede utilizar las siguientes recomendaciones sobre la configuración y las estrategias para optimizar el rendimiento cuando utilice Amazon ECR.

Usar Docker 1.10 o versiones posteriores para poder realizar cargas en capas simultáneas

Las imágenes de Docker se componen de capas, que son etapas intermedias de compilación de la imagen. Cada línea de un archivo Dockerfile genera una nueva capa. Al utilizar Docker 1.10 o versiones posteriores, Docker envía de forma predeterminada tantas capas como cargas simultáneas sea posible enviar a Amazon ECR, lo que da como resultado tiempos de carga más rápidos.

Usar una imagen base más pequeña

Las imágenes predeterminadas disponibles en Docker Hub pueden contener varias dependencias que no son necesarias para la aplicación. Plántese utilizar una imagen más pequeña creada y mantenida por otros miembros de la comunidad Docker o cree su propia imagen base a partir de la imagen de prueba mínima de Docker. Para obtener más información, consulte [Create a base image](#) en la documentación de Docker.

Sitúe las dependencias que menos cambian en la primera parte del archivo Dockerfile

Docker almacena capas en caché, lo que incrementa la velocidad de compilación. Si una capa no ha cambiado desde la última compilación, Docker recurre a la versión en caché en lugar de compilarla de nuevo. Sin embargo, cada capa depende de las que le anteceden. Si una capa cambia, Docker compila de nuevo no solo esa capa, sino también las que le siguen.

Para reducir al mínimo el tiempo necesario para compilar de nuevo un archivo Docker y volver a cargar las capas, plántese situar las dependencias que cambian con menos frecuencia en el archivo Docker. Sitúe las dependencias que cambian rápidamente (como, por ejemplo, el código fuente de la aplicación) más adelante en la pila.

Encadene los comandos para evitar almacenar archivos innecesarios.

Los archivos intermedios que se crean en una capa siguen formando parte de ella aunque se eliminen en una capa posterior. Considere el siguiente ejemplo:

```
WORKDIR /tmp
RUN wget http://example.com/software.tar.gz
RUN wget tar -xvf software.tar.gz
```

```
RUN mv software/binary /opt/bin/myapp
RUN rm software.tar.gz
```

En este ejemplo, las capas creadas por el primer y el segundo comando RUN contienen el archivo original .tar.gz y su contenido descomprimido. Esto ocurre a pesar de que el cuarto comando RUN elimina el archivo .tar.gz. Estos comandos se pueden encadenar en una única instrucción RUN para asegurarse de que los archivos innecesarios no formen parte de la imagen final de Docker:

```
WORKDIR /tmp
RUN wget http://example.com/software.tar.gz &&\
  wget tar -xvf software.tar.gz &&\
  mv software/binary /opt/bin/myapp &&\
  rm software.tar.gz
```

Usar el punto de enlace regional más cercano

Para reducir la latencia al extraer imágenes de Amazon ECR, utilice el punto de enlace regional más cercano a la zona de ejecución de la aplicación. Si la aplicación se ejecuta en una instancia de Amazon EC2, use el siguiente código shell para obtener la región de la zona de disponibilidad de la instancia:

```
REGION=$(curl -s http://169.254.169.254/latest/meta-data/placement/availability-zone
|\
  sed -n 's/\(\d*\)[a-zA-Z]*$/\1/p')
```

La región se puede pasar a AWS CLI los comandos mediante el `--region` parámetro o se puede establecer como la región predeterminada para un perfil mediante el `aws configure` comando. También puedes configurar la región al realizar llamadas con el AWS SDK. Para obtener más información, consulte la documentación del SDK de su lenguaje de programación específico.

Registro privado de Amazon ECR

Los registros privados de Amazon ECR alojan sus imágenes de contenedor en una arquitectura escalable y de alta disponibilidad. Puede utilizar el registro privado para administrar repositorios privados de imágenes que consten de imágenes y artefactos de Docker y Open Container Initiative (OCI). Cada cuenta AWS se proporciona con un registro privado de Amazon ECR predeterminado. Para obtener más información acerca de los registros públicos de Amazon ECR, consulte [Registros públicos](#) en la Guía del usuario de Amazon Elastic Container Registry.

Conceptos de registro privado

- La URL del registro privado predeterminado es `https://aws_account_id.dkr.ecr.us-west-2.amazonaws.com`.
- De forma predeterminada, su cuenta tiene acceso de lectura y escritura en los repositorios que cree en el registro privado. Sin embargo, los usuarios necesitan permisos para realizar llamadas a las API de Amazon ECR y para enviar o extraer imágenes de sus repositorios privados. Amazon ECR proporciona varias políticas administradas para controlar el acceso de los usuarios en distintos niveles. Para obtener más información, consulte [Ejemplos de políticas basadas en identidad de Amazon Elastic Container Registry](#).
- Para poder usar los comandos `docker push` y `docker pull` con objeto de insertar imágenes en los repositorios del registro privado y extraerlas de estos, es necesario autenticar el cliente Docker en ese registro. Para obtener más información, consulte [Autenticación de registro privado en Amazon ECR](#).
- Los repositorios privados se pueden controlar mediante políticas tanto de acceso de usuarios de como de repositorio. Para obtener más información acerca de las políticas de repositorios, consulte [Políticas de repositorios privados en Amazon ECR](#).
- Los repositorios del registro privado se pueden replicar en Regiones de su propio registro privado y en cuentas independientes configurando la replicación para su registro privado. Para obtener más información, consulte [Replicación de imágenes privadas en Amazon ECR](#).

Autenticación de registro privado en Amazon ECR

Puede usar los SDK AWS Management Console AWS CLI, los o los AWS SDK para crear y administrar repositorios privados. También puede utilizar estos métodos para realizar determinadas acciones con las imágenes, por ejemplo listarlas o eliminarlas. Estos clientes utilizan métodos de

AWS autenticación estándar. Aunque es posible usar la API de Amazon ECR para insertar y extraer imágenes, es más probable que use la CLI de Docker o una biblioteca de Docker específica del lenguaje.

La CLI de Docker no admite métodos de autenticación de IAM nativos. Se deben tomar pasos adicionales para que Amazon ECR pueda autenticar y autorizar solicitudes de inserción y extracción de Docker.

Los métodos de autenticación del registro que se detallan en la sección siguiente están disponibles.

Uso del ayudante de credenciales de Amazon ECR

Amazon ECR proporciona un ayudante de credenciales de Docker que hace que sea más fácil almacenar y usar credenciales de Docker cuando se insertan y se extraen imágenes de Amazon ECR. Para obtener información sobre los pasos de instalación y configuración, consulte [Amazon ECR Docker Credential Helper](#).

Note

El asistente de credenciales de Amazon ECR Docker no admite la autenticación multifactor (MFA).

Uso de un token de autorización

El ámbito de permiso de un token de autorización es igual que el de la entidad de seguridad de IAM que se utiliza para recuperar el token de autenticación. Se utiliza un token de autenticación para acceder a un registro de Amazon ECR al que la entidad de seguridad de IAM tiene acceso y que es válido durante 12 horas. Para obtener un token de autorización, debe usar la operación de [GetAuthorizationToken](#) API para recuperar un token de autorización codificado en base64 que contenga el nombre de usuario AWS y una contraseña codificada. El AWS CLI `get-login-password` comando lo simplifica al recuperar y decodificar el token de autorización, que luego puedes canalizar a un comando para autenticarlo. `docker login`

Autenticación de Docker en un registro privado de Amazon ECR con `get-login`

- Para autenticar Docker en un registro de Amazon ECR con `get-login-password`, ejecute el comando. `aws ecr get-login-password` Al pasar el token de autenticación al comando `docker login`, utilice el valor AWS para el nombre de usuario y especifique el URI del registro de Amazon

ECR en el que desea autenticarse. Si se autentica en varios registros, deberá repetir el comando con cada registro.

Important

Si recibe un error, instale o actualice a la versión más reciente de la AWS CLI. Para obtener más información, consulte [Installing the AWS Command Line Interface](#) en la Guía del usuario de AWS Command Line Interface .

- [get-login-password](#) (AWS CLI)

```
aws ecr get-login-password --region region | docker login --username AWS --password-stdin aws_account_id.dkr.ecr.region.amazonaws.com
```

- [Get-ECR \(\) LoginCommand](#) AWS Tools for Windows PowerShell

```
(Get-ECRLoginCommand).Password | docker login --username AWS --password-stdin aws_account_id.dkr.ecr.region.amazonaws.com
```

Uso de la autenticación de la API HTTP

Amazon ECR es compatible con la [API HTTP de Docker Registry](#). No obstante, dado que Amazon ECR es un registro privado, debe proporcionar un token de autorización con cada solicitud HTTP. Puedes añadir un encabezado de autorización HTTP mediante la `-H` opción for curl y pasar el token de autorización proporcionado por el comando. `get-authorization-token` AWS CLI

Autenticación con la API HTTP de Amazon ECR

1. Recupera un token de autorización con AWS CLI y configúralo en una variable de entorno.

```
TOKEN=$(aws ecr get-authorization-token --output text --query 'authorizationData[].authorizationToken')
```

2. Para autenticar en la API, pase la variable `$TOKEN` a la opción `-H` de curl. Por ejemplo, el siguiente comando muestra las etiquetas de imagen de un repositorio de Amazon ECR. Para obtener más información, consulte la documentación de referencia de la [API HTTP de Docker Registry](#).

```
curl -i -H "Authorization: Basic $TOKEN"  
https://aws_account_id.dkr.ecr.region.amazonaws.com/v2/amazonlinux/tags/list
```

La salida es la siguiente:

```
HTTP/1.1 200 OK  
Content-Type: text/plain; charset=utf-8  
Date: Thu, 04 Jan 2018 16:06:59 GMT  
Docker-Distribution-Api-Version: registry/2.0  
Content-Length: 50  
Connection: keep-alive  
  
{"name":"amazonlinux","tags":["2017.09","latest"]}
```

Configuración de registro privado en Amazon ECR

Amazon ECR utiliza configuraciones de registro privado para configurar características de registros. La configuración del registro privado se establece de manera independiente para cada región. Puede utilizar la configuración de registro privado para configurar las siguientes características.

- **Permisos de registro:** una política de permisos de registro proporciona control sobre los permisos de replicación y caché de extracción. Para obtener más información, consulte [Permisos de registro privado en Amazon ECR](#).
- **Reglas de caché de extracción:** puede crear reglas de caché de extracción para almacenar en caché imágenes de un registro público externo de su registro privado de Amazon ECR. Para obtener más información, consulte [Sincronice un registro anterior con un registro privado de Amazon ECR](#).
- **Configuración de replicación:** la configuración de replicación se usa para controlar si los repositorios se copian entre AWS regiones o cuentas. Para obtener más información, consulte [Replicación de imágenes privadas en Amazon ECR](#).
- **Plantillas de creación de repositorios:** una plantilla de creación de repositorios se utiliza para definir la configuración estándar que se aplicará cuando Amazon ECR cree nuevos repositorios en su nombre. Por ejemplo, los repositorios creados mediante una acción de caché de extracción. Para obtener más información, consulte [Plantillas para controlar los repositorios creados durante una acción de extracción de caché](#).

- Configuración de escaneo: de forma predeterminada, el registro tiene el escaneo básico habilitado. Puede habilitar el escaneo mejorado, el cual proporciona un modo de escaneo automático y continuo que analiza las vulnerabilidades del paquete de idiomas de programación y del sistema operativo. Para obtener más información, consulte [Escanee imágenes en busca de vulnerabilidades de software en Amazon ECR](#).

Permisos de registro privado en Amazon ECR

Amazon ECR utiliza una política de registro para conceder permisos a un principal de AWS a nivel de registro privado. Estos permisos se utilizan para abarcar el acceso a la replicación y extraer funciones de caché.

Amazon ECR solo aplica los siguientes permisos a nivel de registro privado. Si se agregan acciones adicionales a la directiva de registro, se producirá un error.

- `ecr:ReplicateImage`: otorga permiso a otra cuenta, denominada registro de origen, para replicar sus imágenes en el registro. Solo se utiliza para la replicación entre cuentas.
- `ecr:BatchImportUpstreamImage`: otorga permiso para recuperar la imagen externa e importarla a su registro privado.
- `ecr:CreateRepository`: otorga permiso para crear un repositorio en un registro privado. Este permiso es necesario si el repositorio donde se conservan las imágenes replicadas o almacenadas en caché no existe todavía en el registro privado.

Note

Si bien es posible añadir la acción `ecr:*` a una política de permisos de registro privado, se considera práctica recomendada agregar únicamente las acciones específicas necesarias en función de la función que esté utilizando en lugar de utilizar un comodín.

Temas

- [Ejemplos de políticas de registro privado para Amazon ECR](#)
- [Concesión de permisos de registro para la replicación entre cuentas en Amazon ECR](#)
- [Otorgar permisos de registro para extraer la memoria caché en Amazon ECR](#)

Ejemplos de políticas de registro privado para Amazon ECR

En los siguientes ejemplos se muestran instrucciones de política de permisos de registro que puede utilizar para controlar los permisos que los usuarios tienen en el registro de Amazon ECR.

Note

En cada ejemplo, si se quita la acción `ecr:CreateRepository` de la instrucción de permisos de registro, la replicación aún puede producirse. No obstante, para que la replicación se realice correctamente, debe crear repositorios con el mismo nombre en su cuenta.

Ejemplo: Permitir al usuario raíz de una cuenta de origen replicar todos los repositorios

La siguiente política de permisos de registro permite al usuario raíz de una cuenta de origen replicar todos los repositorios.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReplicationAccessCrossAccount",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::source_account_id:root"
      },
      "Action": [
        "ecr:CreateRepository",
        "ecr:ReplicateImage"
      ],
      "Resource": [
        "arn:aws:ecr:us-west-2:your_account_id:repository/*"
      ]
    }
  ]
}
```

Ejemplo: permitir que los usuarios root pertenezcan a varias cuentas

La siguiente política de permisos de registro tiene dos declaraciones. Cada sentencia permite al usuario raíz de una cuenta de origen replicar todos los repositorios.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReplicationAccessCrossAccount",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::source_account_id:root"
      },
      "Action": [
        "ecr:CreateRepository",
        "ecr:ReplicateImage"
      ],
      "Resource": [
        "arn:aws:ecr:us-west-2:your_account_id:repository/*"
      ]
    },
    {
      "Sid": "ReplicationAccessCrossAccount",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::source_account_id:root"
      },
      "Action": [
        "ecr:CreateRepository",
        "ecr:ReplicateImage"
      ],
      "Resource": [
        "arn:aws:ecr:us-west-2:your_account_id:repository/*"
      ]
    }
  ]
}
```

Ejemplo: Permitir al usuario raíz de una cuenta de origen replicar todos los repositorios con el prefijo **prod-**.

La siguiente política de permisos de registro permite al usuario raíz de una cuenta de origen replicar todos los repositorios que comiencen por. prod-

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReplicationAccessCrossAccount",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::source_account_id:root"
      },
      "Action": [
        "ecr:CreateRepository",
        "ecr:ReplicateImage"
      ],
      "Resource": [
        "arn:aws:ecr:us-west-2:your_account_id:repository/prod-*"
      ]
    }
  ]
}
```

Concesión de permisos de registro para la replicación entre cuentas en Amazon ECR

El tipo de política de cuentas cruzadas se utiliza para otorgar permisos a una entidad principal AWS , lo que permite la replicación de los repositorios desde un registro de origen a su registro. De forma predeterminada, tiene permiso para configurar la replicación entre regiones en su propio registro. Tan solo necesita configurar la política de registro si concede permiso a otra cuenta para replicar contenido en el registro.

Una política de registro debe conceder permiso para la acción de la API `ecr:ReplicateImage`. Esta es una API de Amazon ECR interna que puede replicar imágenes entre Regiones o cuentas. También puede concederlo para el permiso `ecr:CreateRepository`, que permite a Amazon ECR crear repositorios en el registro si aún no existen. Si no se proporciona el permiso de `ecr:CreateRepository`, en el registro se debe crear manualmente un repositorio con el mismo

nombre que el de origen. Si no se hace nada de esto, la replicación fallará. Todas las acciones fallidas `CreateRepository` o de la `ReplicateImage` API aparecen en CloudTrail.

Para configurar una política de permisos para la replicación (AWS Management Console)

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/>.
2. En la barra de navegación, elija la región en la que se va a configurar la política de registro.
3. En el panel de navegación, elija `Private registry (Registro privado)`, `Registry permissions (Permisos de registro)`.
4. En la página `Registry permissions (Permisos de registro)`, elija `Generate statement (Generar declaración)`.
5. Realice los siguientes pasos para definir la instrucción de política mediante el generador de políticas.
 - a. En `Policy type (Tipo de política)`, elija `Cross account policy (Política entre cuentas)`.
 - b. Para `Statement ID (ID de instrucción)`, ingrese un ID de instrucción único. Este campo se utiliza como `Sid` en la política de registro.
 - c. Para `Accounts (Cuentas)`, ingrese los ID de cuenta de las cuentas a las que quiera conceder permisos. Cuando especifique varios ID de cuenta, sepárelos con una coma.
6. Expanda la sección `Preview policy statement (Vista previa de instrucción de política)` para revisar la instrucción de política de permisos de registro.
7. Una vez confirmada la instrucción de política, elija `Add to policy (Agregar a la política)` para guardar la política en el registro.

Para configurar una política de permisos para la replicación (AWS CLI)

1. Cree un archivo denominado `registry_policy.json` y rellénelo con una política de registro.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReplicationAccessCrossAccount",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::source_account_id:root"
      }
    }
  ],
```

```
    "Action": [
      "ecr:CreateRepository",
      "ecr:ReplicateImage"
    ],
    "Resource": [
      "arn:aws:ecr:us-west-2:your_account_id:repository/*"
    ]
  }
]
```

2. Cree la política de registro mediante el archivo de política.

```
aws ecr put-registry-policy \
  --policy-text file://registry_policy.json \
  --region us-west-2
```

3. Recupere la política de registro que se va a confirmar.

```
aws ecr get-registry-policy \
  --region us-west-2
```

Otorgar permisos de registro para extraer la memoria caché en Amazon ECR

Los permisos de registro privado de Amazon ECR se pueden utilizar para abarcar los permisos de entidades de IAM individuales a fin de utilizar caché de extracción. Si una entidad de IAM tiene más permisos otorgados por una política de IAM de los que la política de permisos de registro concede, prevalece la política de IAM.

Para crear una política de permisos de registro privado (AWS Management Console):

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/>.
2. En la barra de navegación, elija la región en la que configurar su declaración de permisos de registro privado.
3. En el panel de navegación, elija Private registry (Registro privado), Registry permissions (Permisos de registro).
4. En la página Registry permissions (Permisos de registro), elija Generate statement (Generar declaración) .

5. Para cada declaración de política de permisos de caché de extracción que desee crear, haga lo siguiente.
 - a. Para Policy type (Tipo de política), elija Pull through cache policy (Política de caché de extracción).
 - b. Para Statement id (ID de declaración), proporcione un nombre para la política de declaración de caché de extracción.
 - c. Para AM entities (Entidades de IAM), especifique los usuarios, grupos o roles que se deben incluir en la política.
 - d. Para Repository namespace (Espacio de nombres de repositorio), seleccione la regla de caché de extracción a la que asociar la política.
 - e. Para Repository names (Nombres de repositorio), especifique el nombre base del repositorio para el que se va a aplicar la regla. Por ejemplo, si desea especificar el repositorio de Amazon Linux en Amazon ECR Public, el nombre del repositorio sería `amazonlinux`.

Repositorios privados de Amazon ECR

Un repositorio privado de Amazon ECR contiene sus imágenes de Docker, imágenes de Open Container Initiative (OCI) y artefactos compatibles con OCI. Puede crear, supervisar y eliminar repositorios de imágenes y establecer permisos que controlen quién puede acceder a ellos mediante las operaciones de la API de Amazon ECR o la sección Repositorios de la consola de Amazon ECR. Amazon ECR también se integra con la CLI de Docker para que pueda enviar y extraer imágenes de sus entornos de desarrollo a sus repositorios.

Temas

- [Conceptos sobre los repositorios privados](#)
- [Creación de un repositorio privado de Amazon ECR para almacenar imágenes](#)
- [Visualización del contenido y los detalles de un repositorio privado en Amazon ECR](#)
- [Eliminar un repositorio privado en Amazon ECR](#)
- [Políticas de repositorios privados en Amazon ECR](#)
- [Etiquetado de un repositorio privado en Amazon ECR](#)

Conceptos sobre los repositorios privados

- De forma predeterminada, su cuenta tiene acceso de lectura y escritura en los repositorios e imágenes que cree en el registro predeterminado (`aws_account_id.dkr.ecr.region.amazonaws.com`). No obstante, los usuarios necesitan permisos para realizar llamadas a las API de Amazon ECR y para insertar imágenes en los repositorios o extraerlas de ellos. Amazon ECR proporciona varias políticas administradas para controlar el acceso de los usuarios en distintos niveles. Para obtener más información, consulte [Ejemplos de políticas basadas en identidad de Amazon Elastic Container Registry](#).
- Los repositorios se pueden controlar mediante políticas tanto de acceso de usuarios de como de repositorio individuales. Para obtener más información, consulte [Políticas de repositorios privados en Amazon ECR](#).
- Los nombres de repositorio pueden admitir espacios de nombres, que puede usar para agrupar repositorios similares. Por ejemplo, si varios equipos usan el mismo registro, el equipo A puede usar el espacio de nombres `team-a` y el equipo B puede usar el espacio de nombres `team-b`. Al hacer esto, cada equipo tiene su propia imagen, llamada `web-app`, con cada imagen precedida por el espacio de nombres del equipo. Esta configuración permite que estas imágenes en cada

equipo se utilicen simultáneamente sin interferencias. La imagen del equipo A es `team-a/web-app` y la del equipo B es `team-b/web-app`.

- Las imágenes se pueden replicar en otros repositorios entre regiones, en su propio registro, y entre cuentas. Para ello, especifique una configuración de replicación en las opciones del registro. Para obtener más información, consulte [Configuración de registro privado en Amazon ECR](#).

Creación de un repositorio privado de Amazon ECR para almacenar imágenes

Cree un repositorio privado de Amazon ECR y, a continuación, utilícelo para almacenar las imágenes del contenedor. Utilice los siguientes pasos para crear un repositorio privado mediante la AWS Management Console. Para ver los pasos para crear un repositorio mediante el AWS CLI, consulte [Paso 3: crear un repositorio](#).

Creación de un repositorio (AWS Management Console)

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/repositories>.
2. En la barra de navegación, elija la región en la que va a crear el repositorio.
3. En la página Repositorios, selecciona Repositorios privados y, a continuación, selecciona Crear repositorio.
4. En Visibility settings (Configuración de visibilidad), verifique que esté seleccionado Private (Privado).
5. En Repository name (Nombre del repositorio), ingrese un nombre exclusivo para el repositorio. El nombre del repositorio se puede especificar por sí mismo (por ejemplo, `nginx-web-app`). También puede ir precedido de un espacio de nombres para agrupar el repositorio en una categoría (por ejemplo, `project-a/nginx-web-app`).

Note

El nombre del repositorio puede contener un máximo de 256 caracteres. Los nombres deben comenzar por una letra y solo pueden contener letras minúsculas, números, guiones, guiones bajos, puntos y barras inclinadas. No se admite el uso de guiones dobles, guiones bajos o barras oblicuas.

6. En Tag mutability (Mutabilidad de etiquetas), elija la configuración de mutabilidad de etiquetas del repositorio. Los repositorios configurados con etiquetas inmutables impiden que se

- sobrescriban las etiquetas de imagen. Para obtener más información, consulte [Evitar que las etiquetas de imagen se sobrescriban en Amazon ECR](#).
7. En Scan on push (Analizar al insertar), si bien puede especificar la configuración de análisis en el nivel del repositorio para el análisis básico, la práctica recomendada es especificar la configuración de análisis en el nivel del registro privado. Especificar la configuración de análisis en el registro privado permite habilitar el análisis mejorado o el análisis básico, así como definir filtros para especificar qué repositorios se deben analizar. Para obtener más información, consulte [Escanee imágenes en busca de vulnerabilidades de software en Amazon ECR](#).
 8. Para el cifrado de KMS, elija si desea habilitar el cifrado de las imágenes del repositorio mediante AWS Key Management Service. De forma predeterminada, cuando el cifrado KMS está activado, Amazon ECR utiliza una clave administrada de AWS (clave KMS) con el alias `aws/ecr`. Esta clave se crea en su cuenta la primera vez que crea un repositorio con el cifrado de KMS habilitado. Para obtener más información, consulte [Cifrado en reposo](#).
 9. Cuando el cifrado de KMS esté habilitado, seleccione Customer encryption settings (advanced) (Configuración de cifrado de clientes (Avanzado)) para elegir su propia clave KMS. La clave KMS debe estar en la misma región que el clúster. Seleccione Crear una AWS KMS clave para ir a la AWS KMS consola y crear su propia clave.
 10. Elija Create repository.

Siguientes pasos

Para ver los pasos necesarios para insertar una imagen en tu repositorio, selecciona el repositorio y elige Ver comandos de inserción. Para obtener más información sobre cómo insertar una imagen en el repositorio, consulte [Enviar una imagen a un repositorio privado de Amazon ECR](#).

Visualización del contenido y los detalles de un repositorio privado en Amazon ECR

Después de crear un repositorio privado, puede ver los detalles sobre el repositorio en: AWS Management Console

- Qué imágenes están almacenadas en un repositorio
- Detalles de cada imagen almacenada en el repositorio, como el tamaño y el resumen de SHA de cada una
- Frecuencia de análisis especificada para el contenido del repositorio

- Si el repositorio tiene asociada una regla de caché de extracción activa
- Configuración de cifrado del repositorio

Note

A partir de la versión de Docker 1.9, el cliente Docker comprime las capas de las imágenes antes de insertarlas en un registro V2 Docker. La salida del comando `docker images` muestra el tamaño de la imagen sin comprimir. Por lo tanto, tenga en cuenta que Docker podría devolver una imagen más grande que la mostrada en la AWS Management Console.

Visualización de la información del repositorio (AWS Management Console)

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/repositories>.
2. En la barra de navegación, seleccione la región que contiene el repositorio que desea ver.
3. En el panel de navegación, elija Repositories (Repositorios).
4. En la página Repositories (Repositorios), elija la pestaña Private (Privados) y, a continuación, el repositorio que desea ver.
5. En la página de detalles del repositorio, la consola muestra de forma predeterminada la vista Images (Imágenes). Utilice el menú de navegación para ver otro tipo de información sobre el repositorio.
 - Elija Summary (Resumen) para ver los detalles del repositorio y los datos del recuento de extracción del repositorio.
 - Elija Images (Imágenes) para ver información sobre las etiquetas de las imágenes del repositorio. Para ver más información sobre la imagen, seleccione la etiqueta de la imagen. Para obtener más información, consulte [Visualización de los detalles de la imagen en Amazon ECR](#).

Si hay imágenes sin etiquetar que desea eliminar, puede seleccionar la casilla situada a la izquierda de los repositorios que desea eliminar y elegir Delete (Eliminar). Para obtener más información, consulte [Eliminar una imagen en Amazon ECR](#).

 - Elija Permissions (Permisos) para ver las políticas de repositorio que se aplican al repositorio. Para obtener más información, consulte [Políticas de repositorios privados en Amazon ECR](#).

- Elija Lifecycle Policy (Política de ciclo de vida) para ver las reglas de política de ciclo de vida que se aplican al repositorio. El historial de eventos del ciclo de vida también se visualiza aquí. Para obtener más información, consulte [Automatice la limpieza de imágenes mediante políticas de ciclo de vida en Amazon ECR](#).
- Elija Tags (Etiquetas) para ver las etiquetas de metadatos que se aplican al repositorio.

Eliminar un repositorio privado en Amazon ECR

Si ya ha terminado de usar un repositorio, puede eliminarlo. Al eliminar un repositorio del AWS Management Console, también se eliminan todas las imágenes contenidas en el repositorio; esto no se puede deshacer.

Important

Las imágenes de los repositorios eliminados también se eliminan. No podrá deshacer esta operación.

Para eliminar un repositorio (AWS Management Console)

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/repositories>.
2. En la barra de navegación, seleccione la región que contiene el repositorio que desea eliminar.
3. En el panel de navegación, elija Repositories (Repositorios).
4. En la página Repositories (Repositorios), elija la pestaña Private (Privados) y, a continuación, seleccione el repositorio que desea eliminar y elija Delete (Eliminar).
5. En la ventana Delete (Eliminar) **nombre_repositorio**, verifique los repositorios seleccionados que deben eliminarse y elija Delete (Eliminar).

Políticas de repositorios privados en Amazon ECR

Amazon ECR utiliza permisos basados en recursos para controlar el acceso a los repositorios. Los permisos basados en recursos le permiten especificar qué usuarios o roles tienen acceso a un repositorio y qué acciones pueden realizar en él. De forma predeterminada, solo la AWS cuenta que creó el repositorio tiene acceso al repositorio. Puedes aplicar una política de repositorio que permita un acceso adicional a tu repositorio.

Temas

- [Políticas de repositorios frente a políticas de IAM](#)
- [Ejemplos de políticas de repositorios privados en Amazon ECR](#)
- [Configuración de una declaración de política de repositorios privados en Amazon ECR](#)

Políticas de repositorios frente a políticas de IAM

Las políticas de repositorios de Amazon ECR son un subconjunto de políticas de IAM destinados a controlar el acceso a repositorios de Amazon ECR individuales, y se aplican específicamente a este fin. Las políticas de IAM se suelen utilizar para aplicar permisos a todo el servicio de Amazon ECR, pero también se pueden utilizar para controlar el acceso a recursos específicos.

Tanto las políticas de repositorios de Amazon ECR como las políticas de IAM se utilizan a la hora de determinar qué acciones puede realizar un rol o usuario específico en un repositorio. Si se le permite realizar una acción a un rol o usuario mediante una política de repositorio, pero el permiso se deniega mediante una política de IAM (o viceversa), la acción se denegará. Para que un usuario o rol pueda realizar una acción, solo necesita que se le proporcione permiso mediante una política de repositorio o una política de IAM, no de ambas.

Important

Amazon ECR requiere que los usuarios tengan permiso para realizar llamadas a la API `ecr:GetAuthorizationToken` a través de una política de IAM para que puedan autenticarse en un registro, así como insertar o extraer imágenes de cualquier repositorio de Amazon ECR. Amazon ECR proporciona varias políticas de IAM administradas para controlar el acceso de los usuarios en distintos niveles; para obtener más información, consulte [Ejemplos de políticas basadas en identidad de Amazon Elastic Container Registry](#).

Puede utilizar cualquiera de estos tipos de política para controlar el acceso a los repositorios, como se muestra en los siguientes ejemplos.

En este ejemplo se muestra una política de repositorio de Amazon ECR que permite a un usuario específico describir el repositorio y las imágenes que contiene este.

```
{  
  "Version": "2012-10-17",
```

```

"Statement": [
  {
    "Sid": "ECRRepositoryPolicy",
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::account-id:user/username"},
    "Action": [
      "ecr:DescribeImages",
      "ecr:DescribeRepositories"
    ]
  }
]
}

```

En este ejemplo se muestra una política de IAM que logra el mismo objetivo que la anterior al limitar la política a un repositorio (especificado por el ARN completo del repositorio) mediante el parámetro de recurso. Para obtener más información sobre el formato de Nombres de recursos de Amazon (ARN), consulte [Recursos](#).

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowDescribeRepoImage",
      "Effect": "Allow",
      "Action": [
        "ecr:DescribeImages",
        "ecr:DescribeRepositories"
      ],
      "Resource": ["arn:aws:ecr:region:account-id:repository/repository-name"]
    }
  ]
}

```

Ejemplos de políticas de repositorios privados en Amazon ECR

Important

Los ejemplos de políticas de repositorios de esta página están pensados para aplicarse a los repositorios privados de Amazon ECR. No funcionarán correctamente si se utilizan directamente con una entidad principal de IAM, a menos que se modifiquen para especificar el repositorio de Amazon ECR como recurso. Para obtener más información acerca de cómo

establecer políticas de repositorios, consulte [Configuración de una declaración de política de repositorios privados en Amazon ECR](#).

Las políticas de repositorios de Amazon ECR son un subconjunto de políticas de IAM destinados a controlar el acceso a repositorios de Amazon ECR individuales, y se aplican específicamente a este fin. Las políticas de IAM se suelen utilizar para aplicar permisos a todo el servicio de Amazon ECR, pero también se pueden utilizar para controlar el acceso a recursos específicos. Para obtener más información, consulte [Políticas de repositorios frente a políticas de IAM](#).

En los siguientes ejemplos de política de repositorio se muestran instrucciones de permiso que puede utilizar para controlar el acceso a los repositorios privados de Amazon ECR.

Important

Amazon ECR requiere que los usuarios tengan permiso para realizar llamadas a la API `ecr:GetAuthorizationToken` a través de una política de IAM para que puedan autenticarse en un registro, así como insertar o extraer imágenes de cualquier repositorio de Amazon ECR. Amazon ECR proporciona varias políticas de IAM administradas para controlar el acceso de los usuarios en distintos niveles; para obtener más información, consulte [Ejemplos de políticas basadas en identidad de Amazon Elastic Container Registry](#).

Ejemplo: Permitir uno o más usuarios de

La siguiente política de repositorio permite que uno o más usuarios de inserten imágenes en un repositorio y las extraigan de este.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowPushPull",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::account-id:user/push-pull-user-1",
          "arn:aws:iam::account-id:user/push-pull-user-2"
        ]
      }
    }
  ]
}
```

```

    },
    "Action": [
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability",
        "ecr:CompleteLayerUpload",
        "ecr:GetDownloadUrlForLayer",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
    ]
}
]
}

```

Ejemplo: Permitir otra cuenta

La siguiente política de repositorio permite a una cuenta específica insertar imágenes.

Important

La cuenta a la que está otorgando permisos debe tener habilitada la región en la que está creando la política de repositorio; de lo contrario, se producirá un error.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCrossAccountPush",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:root"
      },
      "Action": [
        "ecr:BatchCheckLayerAvailability",
        "ecr:CompleteLayerUpload",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ]
    }
  ]
}

```

```
}

```

La siguiente política de repositorio permite a determinados usuarios extraer imágenes (*pull-user-1* y *pull-user-2*), al tiempo que proporciona acceso completo a otro usuario (*admin-user*).

Note

Para políticas de repositorio más complicadas que actualmente no son compatibles con el AWS Management Console, puede aplicar la política con el [set-repository-policy](#) AWS CLI comando.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowPull",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::account-id:user/pull-user-1",
          "arn:aws:iam::account-id:user/pull-user-2"
        ]
      },
      "Action": [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer"
      ]
    },
    {
      "Sid": "AllowAll",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:user/admin-user"
      },
      "Action": [
        "ecr:*"
      ]
    }
  ]
}
```

```
}

```

Ejemplo: Denegar todo

La siguiente política de repositorio deniega a todos los usuarios de todas las cuentas la capacidad de extraer imágenes.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPull",
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer"
      ]
    }
  ]
}
```

Ejemplo: Restringir el acceso a direcciones IP específicas

El siguiente ejemplo deniega permisos a cualquier usuario para realizar cualquier operación de Amazon ECR cuando se aplica a un repositorio desde un rango específico de direcciones.

La condición en esta declaración identifica el rango 54.240.143.* de direcciones IP permitidas del protocolo de Internet versión 4 (IPv4).

El `Condition` bloque utiliza `NotIpAddress` las condiciones y la clave de `aws:SourceIp` condición, que es una clave de condición que AWS abarca todo el espacio. Para obtener más información sobre estas claves de condición, consulte [Claves de contexto de condición globales de AWS](#). Los valores de IPv4 `aws:sourceIp` utilizan la notación CIDR estándar. Para obtener más información, consulte [Operadores de condición de dirección IP](#) en la guía del usuario de IAM.

```
{
  "Version": "2012-10-17",
  "Id": "ECRPolicyId1",
  "Statement": [
    {
      "Sid": "IPAllow",
```

```

    "Effect": "Deny",
    "Principal": "*",
    "Action": "ecr:*",
    "Condition": {
      "NotIpAddress": {
        "aws:SourceIp": "54.240.143.0/24"
      }
    }
  }
]
}

```

Ejemplo: permitir un servicio AWS

La siguiente política de repositorios permite el AWS CodeBuild acceso a las acciones de la API Amazon ECR necesarias para la integración con ese servicio. Al utilizar el siguiente ejemplo, debe utilizar `aws:SourceArn` y las claves de condición `aws:SourceAccount` para el ámbito de qué recursos pueden asumir estos permisos. Para obtener más información, consulte el [ejemplo de Amazon ECR CodeBuild](#) en la Guía del AWS CodeBuild usuario.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CodeBuildAccess",
      "Effect": "Allow",
      "Principal": {
        "Service": "codebuild.amazonaws.com"
      },
      "Action": [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:codebuild:region:123456789012:project/project-  
name"
        },
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        }
      }
    }
  ]
}

```

```
]
}
```

Configuración de una declaración de política de repositorios privados en Amazon ECR

Puede añadir una declaración de política de acceso a un repositorio AWS Management Console siguiendo los pasos que se indican a continuación. Puede añadir varias instrucciones de política por repositorio. Para ver ejemplos de políticas, consulte [Ejemplos de políticas de repositorios privados en Amazon ECR](#).

Important

Amazon ECR requiere que los usuarios tengan permiso para realizar llamadas a la API `ecr:GetAuthorizationToken` a través de una política de IAM para que puedan autenticarse en un registro, así como insertar o extraer imágenes de cualquier repositorio de Amazon ECR. Amazon ECR proporciona varias políticas de IAM administradas para controlar el acceso de los usuarios en distintos niveles; para obtener más información, consulte [Ejemplos de políticas basadas en identidad de Amazon Elastic Container Registry](#).


Para definir una instrucción de política de repositorio

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/repositories>.
2. En la barra de navegación, seleccione la región que contiene el repositorio para el que desea definir una instrucción de política.
3. En el panel de navegación, elija Repositories (Repositorios).
4. En la página Repositories (Repositorios), elija el repositorio para el que desea definir una instrucción de política con objeto de ver su contenido.
5. En la vista de lista de imágenes del repositorio, en el panel de navegación, elija Permissions (Permisos), Edit (Editar).

Note


Si no ve la opción Permissions (Permisos) en el panel de navegación, asegúrese de que está en la vista de lista de imágenes del repositorio.

6. En la página Edit permissions (Editar permisos), seleccione Add statement (Añadir declaración).
7. En Statement name (Nombre de la declaración), introduzca un nombre para la declaración.
8. En Effect (Efecto), elija si desea que la instrucción de política de como resultado un permiso o una denegación explícita.
9. En Principal (Entidad de seguridad), elija el alcance con el que se va a aplicar la instrucción de la política. Para obtener más información, consulte [Elementos de la política de JSON de AWS : Entidad de servicio](#) en la Guía del usuario de IAM.
 - Puede aplicar la declaración a todos los AWS usuarios autenticados seleccionando la casilla Todos (*).
 - En (Entidad de servicio), especifique el nombre de la entidad de servicio (por ejemplo, ecs.amazonaws.com) para aplicar la instrucción a un servicio específico.
 - En el AWS caso de los ID de AWS cuenta, especifique un número de cuenta (por ejemplo,111122223333) para aplicar la declaración a todos los usuarios de una AWS cuenta específica. Se pueden especificar varias cuentas utilizando una lista delimitada por comas.

 Important

La cuenta a la que está otorgando permisos debe tener habilitada la región en la que está creando la política de repositorio; de lo contrario, se producirá un error.

- En el caso de las entidades de IAM, seleccione las funciones o los usuarios de su AWS cuenta a los que desee aplicar la declaración.

 Note

Para políticas de repositorio más complicadas que actualmente no son compatibles con el AWS Management Console, puede aplicar la política con el [set-repository-policy](#) AWS CLI comando.

10. En Actions (Acciones), elija el alcance de las operaciones de la API de Amazon ECR a las que debe aplicarse la instrucción de la política en la lista de operaciones de API individuales.
11. Cuando haya terminado, elija Save para definir la política.
12. Repita el paso anterior para cada política de repositorio que desee añadir.

Etiquetado de un repositorio privado en Amazon ECR

Para ayudarle a gestionar sus repositorios de Amazon ECR, puede asignar sus propios metadatos a los repositorios de Amazon ECR nuevos o existentes mediante etiquetas de recursos. AWS Por ejemplo, puede definir un conjunto de etiquetas para los repositorios de Amazon ECR de su cuenta que le ayuden a rastrear al propietario de cada repositorio.

Conceptos básicos de etiquetas

Las etiquetas no tienen ningún significado semántico para Amazon ECR, por lo que se interpretan estrictamente como cadenas de caracteres. Además, las etiquetas no se asignan a los recursos automáticamente. Puede editar las claves y los valores de las etiquetas y también puede eliminar etiquetas de un recurso en cualquier momento. Puede establecer el valor de una etiqueta como una cadena vacía, pero no puede asignarle un valor nulo. Si añade una etiqueta con la misma clave que una etiqueta existente en ese recurso, el nuevo valor sobrescribirá al antiguo. Si elimina un recurso, también se eliminará cualquier etiqueta asignada a dicho recurso.

Puede trabajar con etiquetas mediante la consola Amazon ECR AWS CLI, la y la API Amazon ECR.

Con AWS Identity and Access Management (IAM), puede controlar qué usuarios de su AWS cuenta tienen permiso para crear, editar o eliminar etiquetas. Para obtener información sobre las etiquetas en las políticas de IAM, consulte [the section called “Uso del control de acceso basado en etiquetas”](#)

Etiquetado de los recursos para facturación

Las etiquetas que agregue a sus repositorios de Amazon ECR son útiles a la hora de revisar la asignación de costes una vez que las habilite en el informe de uso y costes. Para obtener más información, consulte [Informes de uso de Amazon ECR](#).

Para ver el costo de los recursos combinados, puede organizar la información de facturación basada en los recursos que tienen los mismos valores de clave de etiqueta. Por ejemplo, puede etiquetar varios recursos con un nombre de aplicación específico y luego organizar su información de facturación para ver los costos totales de la aplicación en distintos servicios. Para obtener más información sobre la configuración de un informe de asignación de costes con etiquetas, consulte [Informe de asignación de costes mensual](#) en la Guía del usuario de AWS Billing .

Note

Si acaba de habilitar la realización de informes, los datos correspondientes al mes actual estarán disponibles para su visualización transcurridas 24 horas.

Añadir etiquetas a un repositorio privado en Amazon ECR

Puedes añadir etiquetas a un repositorio privado.

Para obtener información sobre los nombres y las prácticas recomendadas para las etiquetas, consulte [los límites y requisitos de nomenclatura](#) de etiquetas y [las prácticas recomendadas](#) en la Guía del usuario de Tagging AWS Resources.

Añadir etiquetas a un repositorio ()AWS Management Console

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/>.
2. En la barra de navegación, seleccione la región que desea utilizar.
3. En el panel de navegación, elija Repositories (Repositorios).
4. En la página Repositories (Repositorios), active la casilla de verificación situada junto al repositorio que desee etiquetar.
5. En el menú Action (Acción), selecciona Repository tags (Etiquetas de repositorio).
6. En la pestaña Repository tags (Etiquetas de repositorio), seleccione Add tags (Añadir etiquetas), Add tag (Añadir etiqueta).
7. En la página Edit repository tags (Editar etiquetas de repositorio), especifique la clave y el valor de cada etiqueta y, a continuación, elija save (Guardar).

Añadir etiquetas a un repositorio (AWS CLI o API)

Puedes añadir o sobrescribir una o más etiquetas mediante la AWS CLI o una API.

- AWS CLI - [recurso de etiquetas](#)
- Acción de la API - [TagResource](#)

En los siguientes ejemplos se muestra cómo añadir etiquetas mediante AWS CLI.

Ejemplo 1: etiquetar un repositorio

El siguiente comando etiqueta un repositorio.

```
aws ecr tag-resource \  
  --resource-arn arn:aws:ecr:region:account_id:repository/repository_name \  
  --tags Key=stack,Value=dev
```

Ejemplo 2: etiquetar un repositorio con varias etiquetas

El siguiente comando añade tres etiquetas a un repositorio.

```
aws ecr tag-resource \  
  --resource-arn arn:aws:ecr:region:account_id:repository/repository_name \  
  --tags Key=key1,Value=value1 Key=key2,Value=value2 Key=key3,Value=value3
```

Ejemplo 3: Enumerar etiquetas de un repositorio

El siguiente comando muestra las etiquetas asociadas a un repositorio.

```
aws ecr list-tags-for-resource \  
  --resource-arn arn:aws:ecr:region:account_id:repository/repository_name
```

Ejemplo 4: Crear un repositorio y añadir una etiqueta

El siguiente comando crea un repositorio denominado `test-repo` y añade una etiqueta con clave `team` y valor `devs`.

```
aws ecr create-repository \  
  --repository-name test-repo \  
  --tags Key=team,Value=devs
```

Eliminar etiquetas de un repositorio privado en Amazon ECR

Puedes eliminar etiquetas de un repositorio privado.

Para eliminar una etiqueta de un repositorio privado (AWS Management Console)

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/>.
2. En la barra de navegación, seleccione la región que desea utilizar.
3. En la página Repositories (Repositorios), active la casilla de verificación situada junto al repositorio del que desee eliminar una etiqueta.

4. En el menú Action (Acción), selecciona Etiquetas de repositorio.
5. En la página Repository tags (Etiquetas de repositorio), seleccione Edit (Editar).
6. En la página Edit repository tags (Editar etiquetas de repositorio), seleccione Remove (Eliminar) para cada etiqueta que desee eliminar y, a continuación, elija Save (Guardar).

Para eliminar una etiqueta de un repositorio privado (AWS CLI)

Puedes eliminar una o más etiquetas mediante la AWS CLI o una API.

- AWS CLI - Recurso [sin etiquetar](#)
- Acción de la API - [UntagResource](#)

En el siguiente ejemplo, se muestra cómo eliminar una etiqueta de un repositorio mediante AWS CLI.

```
aws ecr untag-resource \  
  --resource-arn arn:aws:ecr:region:account_id:repository/repository_name \  
  --tag-keys tag_key
```

Imágenes privadas en Amazon ECR

Amazon ECR almacena imágenes de Docker, imágenes de Open Container Initiative (OCI) y artefactos compatibles con OCI en repositorios privados. Puede utilizar la CLI de Docker, o su cliente favorito, para insertar imágenes de sus repositorios y extraerlas desde estos.

Temas

- [Enviar una imagen a un repositorio privado de Amazon ECR](#)
- [Firmar una imagen almacenada en un repositorio privado de Amazon ECR](#)
- [Eliminar una firma de un repositorio privado de Amazon ECR](#)
- [Visualización de los detalles de la imagen en Amazon ECR](#)
- [Extraer una imagen a su entorno local desde un repositorio privado de Amazon ECR](#)
- [Extracción de la imagen del contenedor de Amazon Linux](#)
- [Eliminar una imagen en Amazon ECR](#)
- [Volver a etiquetar una imagen en Amazon ECR](#)
- [Evitar que las etiquetas de imagen se sobrescriban en Amazon ECR](#)
- [Compatibilidad con el formato de manifiesto de imagen de contenedor en Amazon ECR](#)
- [Uso de imágenes de Amazon ECR con Amazon ECS](#)
- [Uso de imágenes de Amazon ECR con Amazon EKS](#)

Enviar una imagen a un repositorio privado de Amazon ECR

Puede insertar las imágenes Docker, las listas de manifiesto, las imágenes de Open Container Initiative (OCI) y los artefactos compatibles con OCI a sus repositorios privados.

Amazon ECR también proporciona una forma de replicar las imágenes en otros repositorios. Al especificar una configuración de replicación en la configuración de su registro privado, puede replicar en todas las regiones de su propio registro y en diferentes cuentas. Para obtener más información, consulte [Configuración de registro privado en Amazon ECR](#).

Temas

- [Permisos de IAM para enviar una imagen a un repositorio privado de Amazon ECR](#)
- [Enviar una imagen de Docker a un repositorio privado de Amazon ECR](#)
- [Envío de una imagen de arquitectura múltiple a un repositorio privado de Amazon ECR](#)

- [Envío de un gráfico de Helm a un repositorio privado de Amazon ECR](#)

Permisos de IAM para enviar una imagen a un repositorio privado de Amazon ECR

Los usuarios necesitan permisos de IAM para enviar imágenes a los repositorios privados de Amazon ECR. Siguiendo la práctica recomendada de conceder los privilegios mínimos, puede conceder el acceso a un repositorio específico. También puedes conceder acceso a todos los repositorios.

Un usuario debe autenticarse en cada registro de Amazon ECR al que desee insertar imágenes solicitando un token de autorización. Amazon ECR proporciona varias políticas AWS administradas para controlar el acceso de los usuarios en distintos niveles. Para obtener más información, consulte [AWS políticas gestionadas para Amazon Elastic Container Registry](#).

También puede crear sus propias políticas de IAM. La siguiente política de IAM concede los permisos necesarios para enviar una imagen a un repositorio específico. El repositorio debe especificarse como un Nombre de recurso de Amazon (ARN).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecr:CompleteLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:InitiateLayerUpload",
        "ecr:BatchCheckLayerAvailability",
        "ecr:PutImage"
      ],
      "Resource": "arn:aws:ecr:region:111122223333:repository/repository-name"
    },
    {
      "Effect": "Allow",
      "Action": "ecr:GetAuthorizationToken",
      "Resource": "*"
    }
  ]
}
```

La siguiente política de IAM concede los permisos necesarios para enviar una imagen a todos los repositorios.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecr:CompleteLayerUpload",
        "ecr:GetAuthorizationToken",
        "ecr:UploadLayerPart",
        "ecr:InitiateLayerUpload",
        "ecr:BatchCheckLayerAvailability",
        "ecr:PutImage"
      ],
      "Resource": "*"
    }
  ]
}
```

Enviar una imagen de Docker a un repositorio privado de Amazon ECR

Puede insertar las imágenes de contenedor a un repositorio de Amazon ECR con el comando docker push.

Amazon ECR también admite la creación y el envío de listas de manifiestos de Docker que se utilizan para imágenes de varias arquitecturas. Para obtener más información, consulte [Envío de una imagen de arquitectura múltiple a un repositorio privado de Amazon ECR](#).

Inserción de una imagen de Docker en un repositorio de Amazon ECR

El repositorio de Amazon ECR debe existir antes de insertar la imagen. Para obtener más información, consulte [the section called “Crear un repositorio para almacenar imágenes”](#).

1. Autentique su cliente de Docker en el registro de Amazon ECR en el que va a insertar la imagen. Debe obtener tokens de autenticación para cada registro usado, cuya validez es de 12 horas. Para obtener más información, consulte [Autenticación de registro privado en Amazon ECR](#).

Para autenticar Docker en un registro de Amazon ECR, ejecute el comando `aws ecr get-login-password`. Al pasar el token de autenticación al comando `docker login`, utilice el valor `AWS`

para el nombre de usuario y especifique el URI del registro de Amazon ECR en el que desea autenticarse. Si se autentica en varios registros, deberá repetir el comando con cada registro.

⚠ Important

Si recibe un error, instale o actualice a la versión más reciente de la AWS CLI. Para obtener más información, consulte [Installing the AWS Command Line Interface](#) en la Guía del usuario de AWS Command Line Interface .

```
aws ecr get-login-password --region region | docker login --username AWS --password-stdin aws_account_id.dkr.ecr.region.amazonaws.com
```

2. Si el repositorio de imágenes no existe aún en el registro en el que lo va a insertar, créelo. Para obtener más información, consulte [Creación de un repositorio privado de Amazon ECR para almacenar imágenes](#).
3. Identifique la imagen local que va a insertar. Ejecute el comando `docker images` para mostrar las imágenes de contenedor en el sistema.

```
docker images
```

Puede identificar una imagen con el valor *repositorio:etiqueta* o el ID de imagen en la salida del comando resultante.

4. Etiquete su imagen con la combinación de nombres del registro, repositorio y etiqueta de imagen opcional de Amazon ECR que se van a usar. El formato del registro es *aws_account_id.dkr.ecr.us-west-2.amazonaws.com*. El nombre del repositorio debe coincidir con el repositorio que ha creado para su imagen. Si omite la etiqueta de imagen, se presupone que la etiqueta es `latest`.

En el siguiente ejemplo se etiqueta una imagen local con el ID *e9ae3c220b23* como *aws_account_id.dkr.ecr.us-west-2.amazonaws.com/my-repository:tag*.

```
docker tag e9ae3c220b23 aws_account_id.dkr.ecr.us-west-2.amazonaws.com/my-repository:tag
```

5. Inserte la imagen mediante el comando `docker push`:

```
docker push aws_account_id.dkr.ecr.us-west-2.amazonaws.com/my-repository:tag
```

6. (Opcional) Aplique todas las demás etiquetas a su imagen e insértelas en Amazon ECR repitiendo [Step 4](#) y [Step 5](#).

Envío de una imagen de arquitectura múltiple a un repositorio privado de Amazon ECR

Puede insertar imágenes de varias arquitecturas en un repositorio de Amazon ECR mediante la creación y el envío de listas de manifiestos de Docker. Una lista de manifiesto es una lista de imágenes que se crea especificando uno o más nombres de imagen. En la mayoría de los casos, la lista de manifiestos se crea a partir de imágenes que cumplen la misma función, pero que son para diferentes sistemas operativos o arquitecturas. La lista de manifiesto no es obligatoria. Para obtener más información, consulte [manifiesto de docker](#).

Se puede extraer o hacer referencia a una lista de manifiesto en una definición de tarea de Amazon ECS o especificación de pod de Amazon EKS como otras imágenes de Amazon ECR.

Requisitos previos

- En la CLI de Docker, active las funciones experimentales. Para obtener información sobre las funciones experimentales, consulte [Características experimentales](#) en la documentación de Docker.
- El repositorio de Amazon ECR debe existir antes de insertar la imagen. Para obtener más información, consulte [the section called “Crear un repositorio para almacenar imágenes”](#).
- Las imágenes deben enviarse a tu repositorio antes de crear el manifiesto de Docker. Para obtener información acerca de cómo insertar una imagen, consulte [Enviar una imagen de Docker a un repositorio privado de Amazon ECR](#).

Inserción de una imagen de Docker multiarquitectura a un repositorio de Amazon ECR

1. Autentique su cliente de Docker en el registro de Amazon ECR en el que va a insertar la imagen. Debe obtener tokens de autenticación para cada registro usado, cuya validez es de 12 horas. Para obtener más información, consulte [Autenticación de registro privado en Amazon ECR](#).

Para autenticar Docker en un registro de Amazon ECR, ejecute el comando `aws ecr get-login-password`. Al pasar el token de autenticación al comando `docker login`, utilice el valor `AWS`

para el nombre de usuario y especifique el URI del registro de Amazon ECR en el que desea autenticarse. Si se autentica en varios registros, deberá repetir el comando con cada registro.

⚠ Important

Si recibe un error, instale o actualice a la versión más reciente de la AWS CLI. Para obtener más información, consulte [Installing the AWS Command Line Interface](#) en la Guía del usuario de AWS Command Line Interface .

```
aws ecr get-login-password --region region | docker login --username AWS --password-stdin aws_account_id.dkr.ecr.region.amazonaws.com
```

2. Enumere las imágenes en su repositorio, confirmando las etiquetas de imagen.

```
aws ecr describe-images --repository-name my-repository
```

3. Cree la lista de manifiestos de Docker. El comando `manifest create` verifica que las imágenes a las que se hace referencia ya estén en su repositorio y crea el manifiesto localmente.

```
docker manifest create aws_account_id.dkr.ecr.us-west-2.amazonaws.com/my-repository aws_account_id.dkr.ecr.us-west-2.amazonaws.com/my-repository:image_one_tag aws_account_id.dkr.ecr.us-west-2.amazonaws.com/my-repository:image_two
```

4. (Opcional) Inspeccione la lista de manifiestos de Docker. Esto le permite confirmar el tamaño y la síntesis de cada manifiesto de imagen al que se hace referencia en la lista de manifiestos.

```
docker manifest inspect aws_account_id.dkr.ecr.us-west-2.amazonaws.com/my-repository
```

5. Inserte la lista de manifiesto de Docker en su repositorio de Amazon ECR.

```
docker manifest push aws_account_id.dkr.ecr.us-west-2.amazonaws.com/my-repository
```

Envío de un gráfico de Helm a un repositorio privado de Amazon ECR

Puede enviar artefactos de Open Container Initiative (OCI) a un repositorio de Amazon ECR. Para ver un ejemplo de esta funcionalidad, siga los siguientes pasos para enviar un gráfico de Helm a Amazon ECR.

Para obtener información sobre el uso de sus gráficos de Helm alojados en Amazon ECR con Amazon EKS, consulte [Instalación de un gráfico de Helm en un clúster de Amazon EKS](#).

Inserción de un gráfico de Helm a un repositorio de Amazon ECR

1. Instale la última versión del cliente Helm. Estos pasos se han escrito con la versión 3.8.2 de Helm. Para obtener más información, consulte [Instalación de Helm](#).
2. Complete los pasos siguientes para crear un gráfico de Helm de prueba. Para obtener más información, consulte [Documentación de Helm: Introducción](#).
 - a. Cree un gráfico de Helm llamado `helm-test-chart` y borre el contenido del directorio `templates`.

```
helm create helm-test-chart  
rm -rf ./helm-test-chart/templates/*
```

- b. Cree un ConfigMap en la `templates` carpeta.

```
cd helm-test-chart/templates  
cat <<EOF > configmap.yaml  
apiVersion: v1  
kind: ConfigMap  
metadata:  
  name: helm-test-chart-configmap  
data:  
  myvalue: "Hello World"  
EOF
```

3. Empaquete el gráfico. La salida incluirá el nombre de archivo del gráfico empaquetado que se utiliza al insertar el gráfico de Helm.

```
cd ../../  
helm package helm-test-chart
```

Salida

```
Successfully packaged chart and saved it to: /Users/username/helm-test-chart-0.1.0.tgz
```

4. Cree un repositorio para almacenar el gráfico de Helm. El nombre del repositorio debe coincidir con el que utiliza al crear el gráfico de Helm en el paso 2. Para obtener más información, consulte [Creación de un repositorio privado de Amazon ECR para almacenar imágenes](#).

```
aws ecr create-repository \
  --repository-name helm-test-chart \
  --region us-west-2
```

5. Autentique el cliente Helm en el registro de Amazon ECR en el que tiene previsto insertar el gráfico de Helm. Debe obtener tokens de autenticación para cada registro usado, cuya validez es de 12 horas. Para obtener más información, consulte [Autenticación de registro privado en Amazon ECR](#).

```
aws ecr get-login-password \
  --region us-west-2 | helm registry login \
  --username AWS \
  --password-stdin aws_account_id.dkr.ecr.us-west-2.amazonaws.com
```

6. Inserte el gráfico de Helm con el comando helm push. La salida debe incluir el URI del repositorio de Amazon ECR y el resumen del Algoritmo hash seguro.

```
helm push helm-test-chart-0.1.0.tgz oci://aws_account_id.dkr.ecr.us-west-2.amazonaws.com/
```

7. Describa el gráfico de Helm.

```
aws ecr describe-images \
  --repository-name helm-test-chart \
  --region us-west-2
```

En el resultado, compruebe que el parámetro `artifactMediaType` indica el tipo de artefacto adecuado.

```
{
  "imageDetails": [
    {
      "registryId": "aws_account_id",
```

```
    "repositoryName": "helm-test-chart",
    "imageDigest":
      "sha256:dd8aebdda7df991a0ffe0b3d6c0cf315fd582cd26f9755a347a52adEXAMPLE",
    "imageTags": [
      "0.1.0"
    ],
    "imageSizeInBytes": 1620,
    "imagePushedAt": "2021-09-23T11:39:30-05:00",
    "imageManifestMediaType": "application/vnd.oci.image.manifest.v1+json",
    "artifactMediaType": "application/vnd.cncf.helm.config.v1+json"
  }
]
```

8. (Opcional) Para obtener más pasos, instale el mapa de configuración de Helm y comience a utilizar Amazon EKS. Para obtener más información, consulte [Instalación de un gráfico de Helm en un clúster de Amazon EKS](#).

Firmar una imagen almacenada en un repositorio privado de Amazon ECR

Amazon ECR se integra AWS Signer para proporcionarle una forma de firmar las imágenes de sus contenedores. Puede almacenar tanto las imágenes de contenedor como las firmas en sus repositorios privados.

Consideraciones

Se debe tener en cuenta lo siguiente al utilizar la firma de imágenes de Amazon ECR.

- Las firmas almacenadas en el repositorio se incluyen en la cuota de servicio para el número máximo de imágenes por repositorio. Para obtener más información, consulte [Cuotas de servicio de Amazon ECR](#).
- Cuando se utilizan políticas de ciclo de vida de Amazon ECR, cualquier acción por parte de una regla para eliminar o hacer que caduque un índice de imágenes de OCI provocará que Amazon ECR elimine todas las firmas a las que haga referencia ese índice de imágenes en un plazo de 24 horas.

Requisitos previos

Antes de comenzar, se deben cumplir los siguientes requisitos previos.

- Instalar y configurar la versión más reciente de la AWS CLI. Para obtener más información, consulte [Instalación o actualización de la versión más reciente de la AWS CLI](#) en la Guía del usuario de AWS Command Line Interface .
- Instale la CLI de Notation y el AWS Signer complemento de Notation. Para obtener más información, consulte [Requisitos previos para firmar imágenes de contenedor](#) en la Guía para desarrolladores de AWS Signer .
- Disponer de una imagen de contenedor guardada en un repositorio privado de Amazon ECR para firmarla. Para obtener más información, consulte [Enviar una imagen a un repositorio privado de Amazon ECR](#).

Configurar la autenticación para el cliente Notary

Antes de poder crear una firma mediante la CLI de Notation, debe configurar el cliente para que pueda autenticarse en Amazon ECR. Si tiene Docker instalado en el mismo host en el que instaló el cliente de Notation, Notation reutilizará el mismo método de autenticación que utiliza para el cliente de Docker. Los comandos `login` y `logout` del Docker permitirán que los comandos `sign` y `verify` de Notation usen esas mismas credenciales y no tendrá que autenticar Notation por separado. Para obtener más información sobre la configuración de su cliente de Notation para la autenticación, consulte [Autenticar con registros compatibles con OCI](#) en la documentación de Notary Project

Si no utiliza Docker u otra herramienta que utilice credenciales de Docker, le recomendamos que utilice el Asistente de credenciales de Docker de Amazon ECR como almacén de credenciales. Para obtener más información sobre cómo instalar y configurar el asistente de credenciales de Amazon ECR, consulte el [Asistente de credenciales de Amazon ECR Docker](#).

Firma de una imagen

Los siguientes pasos se pueden emplear para crear los recursos necesarios para firmar una imagen de contenedor y almacenar la firma en un repositorio privado de Amazon ECR. Notation firma las imágenes mediante el resumen.

Para firmar una imagen

1. Cree un perfil de AWS Signer firma mediante la plataforma de Notation-OCI-SHA384-ECDSA firma. Si lo desea, puede especificar un período de validez de la firma mediante el parámetro `--signature-validity-period`. Este valor puede especificarse utilizando DAYS, MONTHS o YEARS. Si no se especifica ningún periodo de validez, se utiliza el valor predeterminado de 135 meses.

```
aws signer put-signing-profile --profile-name ecr_signing_profile --platform-id  
Notation-OCI-SHA384-ECDSA
```

Note

El nombre del perfil de firma solo admite caracteres alfanuméricos y el guion bajo (_).

2. Autentique el cliente de Notation en el registro predeterminado. En el siguiente ejemplo, se utiliza AWS CLI para autenticar la CLI de Notation en un registro privado de Amazon ECR.

```
aws ecr get-login-password --region region | notation login --username AWS --  
password-stdin 111122223333.dkr.ecr.region.amazonaws.com
```

3. Utilice la CLI de Notation para firmar la imagen y especifíquela mediante el nombre del repositorio y el resumen de SHA. Esto crea la firma y la envía al mismo repositorio privado de Amazon ECR donde se encuentre la imagen que se está firmando.

En el siguiente ejemplo, se firma una imagen en el repositorio `curl` con el resumen de SHA `sha256:ca78e5f730f9a789ef8c63bb55275ac12dfb9e8099e6EXAMPLE`.

```
notation  
sign 111122223333.dkr.ecr.region.amazonaws.com/  
curl@sha256:ca78e5f730f9a789ef8c63bb55275ac12dfb9e8099e6EXAMPLE --plugin  
"com.amazonaws.signer.notation.plugin" --id "arn:aws:signer:region:111122223333:/  
signing-profiles/ecrSigningProfileName"
```

Siguientes pasos

Tras firmar la imagen del contenedor, puede verificar la firma localmente. Para obtener instrucciones sobre cómo verificar una imagen, consulta [Verificar una imagen localmente después de iniciar sesión](#) en la Guía AWS Signer para desarrolladores

Eliminar una firma de un repositorio privado de Amazon ECR

Puede eliminar una firma de un repositorio privado de Amazon ECR. Al crear y enviar una firma mediante la CLI de Notation, también se crea un índice de imágenes de OCI en su repositorio de Amazon ECR. La API de Amazon ECR no permite eliminar artefactos o imágenes a los que haga referencia un índice de imágenes de OCI, de modo que las opciones disponibles para limpiar estos artefactos son las siguientes.

- (Recomendado) Puede utilizar la CLI de ORAS para eliminar el artefacto y ORAS se encargará de actualizar o eliminar el índice de imágenes.
- Puede utilizar la API o la consola de Amazon ECR para eliminar el índice de imágenes de OCI en primer lugar y, a continuación, el artefacto al que se haga referencia; por ejemplo, la firma.

Cuando se utiliza el cliente de ORAS para eliminar firmas y otros artefactos de tipo de referencia, ORAS administra el índice de imágenes de OCI. ORAS eliminará primero la referencia al artefacto del índice, y luego eliminará el manifiesto. Se puede utilizar el comando `oras manifest delete` para hacer referencia al índice del artefacto de la firma.

Para eliminar una firma mediante la CLI ORAS

1. Instale y configure el cliente ORAS.

Para obtener información sobre la instalación y configuración del cliente ORAS, consulte [Instalación](#) en la documentación de ORAS.

2. Para eliminar una firma mediante la CLI ORAS, ejecute el siguiente comando:

```
oras manifest
delete 111122223333.dkr.ecr.region.amazonaws.com/
repository_name@sha256:ca78e5f730f9a789ef8c63bb55275ac12dfb9e8099e6EXAMPLE
```

Visualización de los detalles de la imagen en Amazon ECR

Después de enviar una imagen a su repositorio, puede ver la información sobre ella. Los detalles incluidos son los siguientes:

- URI de imagen
- Etiquetas de la imagen
- Tipo de medio del artefacto
- Tipo de manifiesto de imagen
- Estado de escaneo
- Tamaño de la imagen en MB
- Si la imagen se insertó en el repositorio
- Estado de la replicación

Visualización de los detalles de la imagen (AWS Management Console)

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/repositories>.
2. En la barra de navegación, elija la región que contiene el repositorio que incluye la imagen.
3. En el panel de navegación, elija Repositories (Repositorios).
4. En la página Repositories (Repositorios), elija el repositorio que desea ver.
5. En la página Repositories: **repository_name** (Repositorios: nombre_repositorio), elija la imagen cuyos detalles desea ver.

Extraer una imagen a su entorno local desde un repositorio privado de Amazon ECR

Si desea ejecutar una imagen de Docker que está disponible en Amazon ECR, puede extraerla a su entorno local con el comando `docker pull`. Puede hacerlo desde su registro predeterminado o desde un registro asociado a otra AWS cuenta.

Para utilizar una imagen de Amazon ECR en una definición de tarea de Amazon ECS, consulte [Uso de imágenes de Amazon ECR con Amazon ECS](#).

⚠ Important

Amazon ECR requiere que los usuarios tengan permiso para realizar llamadas a la API `ecr:GetAuthorizationToken` a través de una política de IAM para que puedan autenticarse en un registro, así como insertar o extraer imágenes de cualquier repositorio de Amazon ECR. Amazon ECR proporciona varias políticas AWS administradas para controlar el acceso de los usuarios en distintos niveles. Para obtener información sobre las políticas AWS gestionadas de Amazon ECR, consulte [AWS políticas gestionadas para Amazon Elastic Container Registry](#).

Extracción de una imagen de Docker de un repositorio de Amazon ECR

1. Autentique su cliente de Docker en el registro de Amazon ECR del que va a extraer la imagen. Debe obtener tokens de autenticación para cada registro usado, cuya validez es de 12 horas. Para obtener más información, consulte [Autenticación de registro privado en Amazon ECR](#).
2. (Opcional) Identifique la imagen que va a extraer.
 - Puede mostrar los repositorios de un registro con el comando: `aws ecr describe-repositories`.

```
aws ecr describe-repositories
```

El registro de ejemplo anterior tiene un repositorio llamado `amazonlinux`.

- Puede describir las imágenes de un repositorio con el comando: `aws ecr describe-images`.

```
aws ecr describe-images --repository-name amazonlinux
```

El repositorio de ejemplo anterior tiene una imagen etiquetada como `latest` y `2016.09`, con el resumen de imagen

```
sha256:f1d4ae3f7261a72e98c6ebefe9985cf10a0ea5bd762585a43e0700ed99863807.
```

3. Extraiga la imagen con el comando `docker pull`. El formato del nombre de imagen debe ser `registry/repository[:tag]` para extraer la imagen por etiqueta o `registry/repository[@digest]` para extraerla por resumen.

```
docker pull aws_account_id.dkr.ecr.us-west-2.amazonaws.com/amazonlinux:latest
```

⚠ Important

Si aparece un error `repository-url not found: does not exist or no pull access`, es posible que tenga que autenticar su cliente de Docker con Amazon ECR. Para obtener más información, consulte [Autenticación de registro privado en Amazon ECR](#).

Extracción de la imagen del contenedor de Amazon Linux

La imagen de contenedor de Amazon Linux se construye desde los mismos componentes de software que se incluyen en la AMI de Amazon Linux. La imagen del contenedor de Amazon Linux está disponible para su uso en cualquier entorno como imagen base para las cargas de trabajo de Docker. Si utiliza la AMI de Amazon Linux para las aplicaciones de Amazon EC2, puede contenerizar las aplicaciones con la imagen del contenedor de Amazon Linux.

Puede usar la imagen del contenedor de Amazon Linux en su entorno de desarrollo local y, a continuación, hacer que su aplicación AWS utilice Amazon ECS. Para obtener más información, consulte [Uso de imágenes de Amazon ECR con Amazon ECS](#).

La imagen de contenedor de Amazon Linux está disponible en Amazon ECR Public y en [Docker Hub](#). Para obtener soporte para la imagen del contenedor de Amazon Linux, visita los [foros de AWS desarrolladores](#).

Extracción de la imagen de contenedor de Amazon Linux desde Amazon ECR Public

1. Autentique el cliente Docker en su registro de Amazon Linux Public. Los tokens de autenticación son válidos durante 12 horas. Para obtener más información, consulte [Autenticación de registro privado en Amazon ECR](#).

ℹ Note

Los comandos `ecr-public` están disponibles en la AWS CLI a partir de la versión 1.18.1.187, sin embargo, recomendamos utilizar la versión más reciente de la AWS CLI. Para obtener más información, consulte [Installing the AWS Command Line Interface](#) en la Guía del usuario de AWS Command Line Interface .

```
aws ecr-public get-login-password --region us-east-1 | docker login --username AWS
--password-stdin public.ecr.aws
```

La salida es la siguiente:

```
Login succeeded
```

2. Extraiga la imagen de contenedor de Amazon Linux con el comando `docker pull`. Para ver la imagen de contenedor de Amazon Linux en la galería pública de Amazon ECR, consulte [Galería pública de Amazon ECR: amazonlinux](#).

```
docker pull public.ecr.aws/amazonlinux/amazonlinux:latest
```

3. (Opcional) Ejecute el contenedor localmente.

```
docker run -it public.ecr.aws/amazonlinux/amazonlinux /bin/bash
```

Extracción de la imagen del contenedor de Amazon Linux de Docker Hub

1. Extraiga la imagen de contenedor de Amazon Linux con el comando `docker pull`.

```
docker pull amazonlinux
```

2. (Opcional) Ejecute el contenedor localmente.

```
docker run -it amazonlinux:latest /bin/bash
```

Eliminar una imagen en Amazon ECR

Si ha terminado de usar una imagen, puede eliminarla del repositorio. Si ha terminado de usar un repositorio, puede eliminar todo el repositorio y todas las imágenes que este contiene. Para obtener más información, consulte [Eliminar un repositorio privado en Amazon ECR](#).

Como alternativa a eliminar imágenes manualmente, puede crear políticas de ciclo de vida del repositorio que proporcionen más control sobre la administración del ciclo de vida de las imágenes en sus repositorios. Las políticas de ciclo de vida automatizan este proceso automáticamente. Para

obtener más información, consulte [Automatice la limpieza de imágenes mediante políticas de ciclo de vida en Amazon ECR](#).

Eliminación de una imagen (AWS Management Console)

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/repositories>.
2. En la barra de navegación, seleccione la región que contiene la imagen que desea eliminar.
3. En el panel de navegación, elija Repositories (Repositorios).
4. En la página Repositories, elija el repositorio del que contiene la imagen que desea eliminar.
5. En la página Repositorios: **nombre_repositorio**, seleccione la casilla situada a la izquierda de la imagen que desea eliminar y elija Eliminar.
6. En el cuadro de diálogo Eliminar imágenes, verifique las imágenes seleccionadas que deben eliminarse y elija Eliminar.

Eliminación de una imagen (AWS CLI)

1. Muestre una lista de las imágenes en el repositorio. Las imágenes etiquetadas tendrán un resumen de imagen y una lista de etiquetas asociadas. Las imágenes sin etiquetar solo tendrán un resumen de imagen.

```
aws ecr list-images \  
  --repository-name my-repo
```

2. (Opcional) Elimine las etiquetas de la imagen que no desee especificando la etiqueta asociada a la imagen que desea eliminar. La imagen se elimina cuando se elimina la última etiqueta de esta.

```
aws ecr batch-delete-image \  
  --repository-name my-repo \  
  --image-ids imageTag=tag1 imageTag=tag2
```

3. Elimine una imagen etiquetada o sin etiquetar especificando el resumen de imagen. Al eliminar una imagen haciendo referencia a su resumen, se elimina la imagen y todas sus etiquetas.

```
aws ecr batch-delete-image \  
  --repository-name my-repo \  
  --image-ids imageDigest=sha256:4f70ef7a4d29e8c0c302b13e25962d8f7a0bd304EXAMPLE
```

Para eliminar varias imágenes, puede especificar varias etiquetas de imagen o resúmenes de imagen en la solicitud.

```
aws ecr batch-delete-image \  
  --repository-name my-repo \  
  --image-ids imageDigest=sha256:4f70ef7a4d29e8c0c302b13e25962d8f7a0bd304EXAMPLE  
  imageDigest=sha256:f5t0e245ssffc302b13e25962d8f7a0bd304EXAMPLE
```

Volver a etiquetar una imagen en Amazon ECR

Con las imágenes de Docker Image Manifest V2 Schema 2 puede usar la opción `--image-tag` del comando `put-image` para volver a etiquetar una imagen existente. Puede volver a etiquetar sin extraer o insertar la imagen con Docker. Para imágenes grandes, este proceso ahorra una cantidad considerable de ancho de banda de la red y del tiempo necesario para volver a etiquetar una imagen.

Para volver a etiquetar una imagen (AWS CLI)

Para volver a etiquetar una imagen con AWS CLI

1. Utilice el comando `batch-get-image` para obtener el manifiesto de la imagen para volver a etiquetarla y escribirla en un archivo. En este ejemplo, el manifiesto de una imagen con la etiqueta *latest*, en el repositorio *amazonlinux*, se escribe en una variable de entorno *MANIFEST*.

```
MANIFEST=$(aws ecr batch-get-image --repository-name amazonlinux --image-ids  
  imageTag=latest --output text --query 'images[].imageManifest')
```

2. Use la opción `--image-tag` del comando `put-image` para colocar el manifiesto de imagen en Amazon ECR con una nueva etiqueta. En este ejemplo, la imagen está etiquetada como *2017.03*.

Note

Si la `--image-tag` opción no está disponible en su versión AWS CLI, actualícela a la versión más reciente. Para obtener más información, consulte [Installing the AWS Command Line Interface](#) en la Guía del usuario de AWS Command Line Interface .

```
aws ecr put-image --repository-name amazonlinux --image-tag 2017.03 --image-manifest "$MANIFEST"
```

3. Verifique que la nueva etiqueta de imagen está asociada a la imagen. En la salida siguiente, la imagen tiene las etiquetas `latest` y `2017.03`.

```
aws ecr describe-images --repository-name amazonlinux
```

La salida es la siguiente:

```
{
  "imageDetails": [
    {
      "imageSizeInBytes": 98755613,
      "imageDigest":
"sha256:8d00af8f076eb15a33019c2a3e7f1f655375681c4e5be157a26EXAMPLE",
      "imageTags": [
        "latest",
        "2017.03"
      ],
      "registryId": "aws_account_id",
      "repositoryName": "amazonlinux",
      "imagePushedAt": 1499287667.0
    }
  ]
}
```

Para volver a etiquetar una imagen (AWS Tools for Windows PowerShell)

Para volver a etiquetar una imagen con la AWS Tools for Windows PowerShell

1. Use el cmdlet `Get-ECRImageBatch` para obtener la descripción de la imagen que va a volver a etiquetar y escribirla en una variable de entorno. En este ejemplo, una imagen con la etiqueta `latest`, en el repositorio `amazonlinux`, se escribe en la variable de entorno `$Image`.

Note

Si el cmdlet `Get-ECRIImageBatch` no está disponible en su sistema, consulte [Configuración de AWS Tools for Windows PowerShell](#) en la Guía del usuario de AWS Tools for Windows PowerShell .

```
$Image = Get-ECRIImageBatch -ImageId @{ imageTag="latest" } -
RepositoryName amazonlinux
```

2. Escriba el manifiesto de la imagen en la variable de entorno `$Manifest`.

```
$Manifest = $Image.Images[0].ImageManifest
```

3. Use la opción `-ImageTag` del cmdlet `Write-ECRIImage` para colocar el manifiesto de imagen en Amazon ECR con una nueva etiqueta. En este ejemplo, la imagen está etiquetada como `2017.09`.

```
Write-ECRIImage -RepositoryName amazonlinux -ImageManifest $Manifest -
ImageTag 2017.09
```

4. Verifique que la nueva etiqueta de imagen está asociada a la imagen. En la salida siguiente, la imagen tiene las etiquetas `latest` y `2017.09`.

```
Get-ECRIImage -RepositoryName amazonlinux
```

La salida es la siguiente:

ImageDigest	ImageTag
-----	-----
sha256:359b948ea8866817e94765822787cd482279eed0c17bc674a7707f4256d5d497	latest
sha256:359b948ea8866817e94765822787cd482279eed0c17bc674a7707f4256d5d497	2017.09

Evitar que las etiquetas de imagen se sobrescriban en Amazon ECR

Puede evitar que las etiquetas de imagen se sobrescriban activando la inmutabilidad de las etiquetas en un repositorio. Una vez activada la inmutabilidad de las etiquetas, se devuelve el `ImageTagAlreadyExistsException` error si insertas una imagen con una etiqueta que ya está en el repositorio. La inmutabilidad de las etiquetas afecta a todas las etiquetas. No puedes hacer que algunas etiquetas sean inmutables mientras que otras no.

Puedes usar las AWS CLI herramientas AWS Management Console y para configurar la mutabilidad de las etiquetas de imagen en un repositorio nuevo o en uno existente. Para crear un repositorio siguiendo los pasos de la consola, consulte [Creación de un repositorio privado de Amazon ECR para almacenar imágenes](#).

Configurar la mutabilidad de las etiquetas de imagen ()AWS Management Console

Para configurar la mutabilidad de la etiqueta de imagen

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/repositories>.
2. En la barra de navegación, elija la región que contiene el repositorio que desea editar.
3. En el panel de navegación, elija Repositories (Repositorios).
4. En la página Repositories (Repositorios), elija la pestaña Private (Privados) y, a continuación, seleccione el repositorio que desea editar y elija Edit (Editar).
5. En Tag mutability (Mutabilidad de etiquetas), elija la configuración de mutabilidad de etiquetas del repositorio. Los repositorios configurados con etiquetas inmutables impiden que se sobrescriban las etiquetas de imagen. Para obtener más información, consulte [Evitar que las etiquetas de imagen se sobrescriban en Amazon ECR](#).
6. En Image scan settings (Configuración de análisis de imágenes), si bien puede especificar la configuración de análisis en el nivel del repositorio para el análisis básico, la práctica recomendada es especificar la configuración de análisis en el nivel del registro privado. Especificar la configuración de análisis en el registro privado permite habilitar el análisis mejorado o el análisis básico, así como definir filtros para especificar qué repositorios se deben analizar. Para obtener más información, consulte [Escanee imágenes en busca de vulnerabilidades de software en Amazon ECR](#).

7. Encryption settings (Configuración de cifrado) es un campo solo de visualización, ya que la configuración de cifrado de un repositorio no se puede cambiar una vez que se ha creado el repositorio.
8. Seleccione Save (Guardar) para actualizar la configuración del repositorio.

Establecer la mutabilidad de la etiqueta de imagen (AWS CLI)

Para crear un repositorio con etiquetas inmutables configuradas

Utilice uno de los siguientes comandos para crear un nuevo repositorio de imágenes con etiquetas inmutables configuradas.

- [create-repository](#) (AWS CLI)

```
aws ecr create-repository --repository-name name --image-tag-mutability IMMUTABLE --region us-east-2
```

- [New-ECRRepository](#) (AWS Tools for Windows PowerShell)

```
New-ECRRepository -RepositoryName name -ImageTagMutability IMMUTABLE -Region us-east-2 -Force
```

Para actualizar la configuración de mutabilidad de las etiquetas de imagen de un repositorio

Utilice uno de los siguientes comandos para actualizar la configuración de mutabilidad de las etiquetas de imagen en un repositorio existente.

- [put-image-tag-mutability](#) (AWS CLI)

```
aws ecr put-image-tag-mutability --repository-name name --image-tag-mutability IMMUTABLE --region us-east-2
```

- Mutabilidad de [Write-ECR ImageTag](#) (AWS Tools for Windows PowerShell)

```
Write-ECRImageTagMutability -RepositoryName name -ImageTagMutability IMMUTABLE -Region us-east-2 -Force
```

Compatibilidad con el formato de manifiesto de imagen de contenedor en Amazon ECR

Amazon ECR admite los siguientes formatos del manifiesto de imagen de contenedor:

- Docker Image Manifest V2 Schema 1 (usado con Docker versión 1.9 y anteriores)
- Docker Image Manifest V2 Schema 2 (usado con Docker versión 1.10 y posteriores)
- Especificaciones de la iniciativa de contenedores abiertos (OCI) (versión 1.0 y posteriores)

La compatibilidad con Docker Image Manifest V2 Schema 2 ofrece la siguiente funcionalidad:

- La capacidad de usar varias etiquetas para una imagen singular.
- Posibilidad de almacenar imágenes de contenedores Windows.

Conversión del manifiesto de imagen de Amazon ECR

Cuando inserta imágenes en Amazon ECR y las extrae desde él, el cliente del motor de contenedores (por ejemplo, Docker) se comunica con el registro para aceptar un formato de manifiesto que entiendan tanto el cliente como el registro para usarlo con la imagen.

Cuando inserta una imagen en Amazon ECR con Docker, versión 1.9 o anterior, el formato del manifiesto de imagen se almacena como Docker Image Manifest V2 Schema 1. Cuando inserta una imagen en Amazon ECR con Docker, versión 1.10 o una posterior, el formato del manifiesto de imagen se almacena como Docker Image Manifest V2 Schema 2.

Cuando extrae una imagen de Amazon ECR por etiqueta, este devuelve el formato del manifiesto de imagen almacenado en el repositorio. El formato se devuelve solo si el cliente entiende dicho formato. Si el cliente no entiende el formato del manifiesto de imagen almacenado, Amazon ECR convierte el manifiesto de imagen en un formato comprensible. Por ejemplo, si un cliente Docker 1.9 solicita un manifiesto de imagen que está almacenado como Docker Image Manifest V2 Schema 2, Amazon ECR devuelve el manifiesto en el formato Docker Image Manifest V2 Schema 1. En la tabla siguiente se describen las conversiones disponibles que admite Amazon ECR cuando se extrae una imagen por etiqueta:

Esquema solicitado por el cliente	Insertado en ECR como V2, esquema 1	Insertado en ECR como V2, esquema 2	Insertado en ECR como OCI
V2, esquema 1	No se requiere ninguna conversión	Convertido en V2, esquema 1	Convertido en V2, esquema 1
V2, esquema 2	No hay ninguna conversión disponible; el cliente utiliza V2, esquema 1	No se requiere ninguna conversión	Convertido en V2, esquema 2
OCI	No hay ninguna conversión disponible	Convertido en OCI	No se requiere ninguna conversión

Important

Si extrae una imagen por resumen, no hay ninguna conversión disponible. El cliente debe entender el formato del manifiesto de imagen almacenado en Amazon ECR. Si solicita una imagen Docker Image Manifest V2 Schema 2 por resumen en un cliente Docker 1.9 o anterior, no se puede extraer la imagen. Para obtener más información, consulte [Registry compatibility](#) en la documentación de Docker.

En este ejemplo, si solicita la misma imagen por etiqueta, Amazon ECR convierte el manifiesto de imagen en un formato que el cliente pueda entender. La imagen se extrae correctamente.

Uso de imágenes de Amazon ECR con Amazon ECS

Puede utilizar los repositorios privados de Amazon ECR para alojar imágenes de contenedor y artefactos desde los que puedan realizar extracciones las tareas de Amazon ECS. Para que esto funcione, el agente de contenedor de Amazon ECS o Fargate debe tener permisos para crear las API `ecr:BatchGetImage`, `ecr:GetDownloadUrlForLayer` y `ecr:GetAuthorizationToken`.

Permisos de IAM necesarios

En la siguiente tabla se muestra el rol de IAM que se debe utilizar para cada tipo de lanzamiento que proporciona los permisos necesarios para que las tareas puedan realizar extracciones desde un

repositorio privado de Amazon ECR. Amazon ECS proporciona políticas de IAM administradas que incluyen los permisos necesarios.

Tipo de lanzamiento	Rol de IAM	AWS política de IAM gestionada
Amazon ECS en instancias de Amazon EC2	Utilice el rol de IAM de instancia de contenedor, que está asociado a la instancia de Amazon EC2 registrada en el clúster de Amazon ECS. Para obtener más información, consulte Rol de IAM de instancia de contenedor en la Guía para desarrolladores de Amazon Elastic Container Service.	AmazonEC2ContainerServiceforEC2Role Para obtener más información, consulte AmazonEC2ContainerServiceforEC2Role en la Guía para desarrolladores de Amazon Elastic Container Service.
Amazon ECS alojado en Fargate	Utilice el rol de IAM de ejecución de tareas al que haga referencia en la definición de la tarea de Amazon ECS. Para obtener más información, consulte Rol de IAM de ejecución de tareas en la Guía para desarrolladores de Amazon Elastic Container Service.	AmazonECSTaskExecutionRolePolicy Para obtener más información, consulte AmazonECSTaskExecutionRolePolicy en la Guía para desarrolladores de Amazon Elastic Container Service.
Amazon ECS en instancias externas	Utilice el rol de IAM de instancia de contenedor, que está asociado al servidor ubicado en las instalaciones o la máquina virtual (VM) registrados en el clúster de Amazon ECS. Para obtener más información, consulte	AmazonEC2ContainerServiceforEC2Role Para obtener más información, consulte AmazonEC2ContainerServiceforEC2Role en la Guía para desarrolladores de Amazon Elastic Container Service.

Tipo de lanzamiento	Rol de IAM	AWS política de IAM gestionada
	Rol de IAM de instancia de contenedor de Amazon ECS en la Guía para desarrolladores de Amazon Elastic Container Service.	

Important

Las políticas de IAM AWS gestionadas contienen permisos adicionales que quizás no necesite para su uso. En tal caso, estos son los permisos mínimos necesarios para realizar extracciones desde un repositorio privado de Amazon ECR.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetAuthorizationToken"
      ],
      "Resource": "*"
    }
  ]
}
```

Especificación de una imagen de Amazon ECR en una definición de tarea de Amazon ECS

Cuando se crea una definición de tarea de Amazon ECS, se puede especificar una imagen de contenedor alojada en un repositorio privado de Amazon ECR. En la definición de tarea, asegúrese de utilizar la nomenclatura de `registry/repository:tag` completa para las imágenes de

Amazon ECR. Por ejemplo, `aws_account_id.dkr.ecr.region.amazonaws.com/my-repository:latest`.

El siguiente fragmento de definición de tarea muestra la sintaxis que debería utilizar para especificar una imagen de contenedor alojada en Amazon ECR en la definición de tarea de Amazon ECS.

```
{
  "family": "task-definition-name",
  ...
  "containerDefinitions": [
    {
      "name": "container-name",
      "image": "aws_account_id.dkr.ecr.region.amazonaws.com/my-
repository:latest",
      ...
    }
  ],
  ...
}
```

Uso de imágenes de Amazon ECR con Amazon EKS

Puede utilizar sus imágenes de Amazon ECR con Amazon EKS.

Al hacer referencia a una imagen desde Amazon ECR, debe usar el nombre completo `registry/repository:tag` para la imagen. Por ejemplo, `aws_account_id.dkr.ecr.region.amazonaws.com/my-repository:latest`.

Permisos de IAM necesarios

Si tiene cargas de trabajo de Amazon EKS alojadas en nodos gestionados, nodos autogestionados o AWS Fargate consulte lo siguiente:

- Cargas de trabajo de Amazon EKS alojadas en nodos gestionados o autogestionados: se requiere el rol de IAM del nodo de trabajo de Amazon EKS (`NodeInstanceRole`). El rol de IAM de nodo de trabajo de Amazon EKS debe contener los siguientes permisos de política de IAM para Amazon ECR.

```
{
  "Version": "2012-10-17",
```

```
"Statement": [  
  {  
    "Effect": "Allow",  
    "Action": [  
      "ecr:BatchCheckLayerAvailability",  
      "ecr:BatchGetImage",  
      "ecr:GetDownloadUrlForLayer",  
      "ecr:GetAuthorizationToken"  
    ],  
    "Resource": "*"   
  }  
]
```

Note

Si utilizó `eksctl` o las AWS CloudFormation plantillas de [Getting Started with Amazon EKS](#) para crear sus grupos de clústeres y nodos de trabajo, estos permisos de IAM se aplican a su función de IAM de nodo de trabajo de forma predeterminada.

- Cargas de trabajo de Amazon EKS alojadas en AWS Fargate: utilice la función de ejecución de pods de Fargate, que permite a los pods extraer imágenes de repositorios privados de Amazon ECR. Para obtener más información, consulte [Create a Fargate pod execution role](#) Creación de un rol de ejecución de Fargate.

Instalación de un gráfico de Helm en un clúster de Amazon EKS

Los gráficos de Helm alojados en Amazon ECR se pueden instalar en sus clústeres de Amazon EKS.

Requisitos previos

- Instale la última versión del cliente Helm. Estos pasos se han escrito con la versión 3.9.0 de Helm. Para obtener más información, consulte [Instalación de Helm](#).
- Tiene al menos una versión 1.23.9 o 2.6.3 del AWS CLI instalada en el equipo. Para obtener más información, consulte [Instalación o actualización de la última versión del AWS CLI](#).
- Ha insertado un gráfico de Helm en el repositorio de Amazon ECR. Para obtener más información, consulte [Envío de un gráfico de Helm a un repositorio privado de Amazon ECR](#).
- Ha configurado `kubectl` para que funcione con Amazon EKS. Para obtener más información, consulte [Creación de un elemento kubeconfig para Amazon EKS](#) en la Guía del usuario de

Amazon EKS. Si los siguientes comandos se realizan correctamente para su clúster, entonces tiene la configuración correcta.

```
kubectl get svc
```

Para instalar un gráfico de Helm en un clúster de Amazon EKS

1. Autentique su cliente Helm en el registro de Amazon ECR en el que esté alojado el gráfico de Helm. Debe obtener tokens de autenticación para cada registro usado, cuya validez es de 12 horas. Para obtener más información, consulte [Autenticación de registro privado en Amazon ECR](#).

```
aws ecr get-login-password \  
  --region us-west-2 | helm registry login \  
  --username AWS \  
  --password-stdin aws_account_id.dkr.ecr.region.amazonaws.com
```

2. Instale el gráfico. *helm-test-chart* Reemplácelo por su repositorio y *0.1.0* por la etiqueta de su gráfico de Helm.

```
helm install ecr-chart-demo oci://aws_account_id.dkr.ecr.region.amazonaws.com/helm-test-chart --version 0.1.0
```

La salida debe ser parecida a la siguiente:

```
NAME: ecr-chart-demo  
LAST DEPLOYED: Tue May 31 17:38:56 2022  
NAMESPACE: default  
STATUS: deployed  
REVISION: 1  
TEST SUITE: None
```

3. Verifique la instalación del gráfico.

```
helm list -n default
```

Ejemplo de salida:

NAME	NAMESPACE	REVISION	UPDATED
STATUS	CHART		APP VERSION
ecr-chart-demo	default	1	2022-06-01 15:56:40.128669157 +0000
UTC deployed	helm-test-chart-0.1.0	1.16.0	

- (Opcional) Consulte el ConfigMap del gráfico de Helm instalado.

```
kubectl describe configmap helm-test-chart-configmap
```

- Cuando haya terminado, puede quitar la versión del gráfico del clúster.

```
helm uninstall ecr-chart-demo
```

Escanee imágenes en busca de vulnerabilidades de software en Amazon ECR

La función de digitalización básica mejorada se encuentra en la versión preliminar de Amazon ECR y está sujeta a cambios. Durante esta versión preliminar pública, solo podrá utilizarla para suscribirse AWS Management Console a la versión de digitalización básica mejorada.

El escaneo de imágenes de Amazon ECR ayuda a identificar las vulnerabilidades de software en las imágenes de sus contenedores. Se ofrecen los siguientes tipos de escaneo:

Important

Al cambiar entre las versiones de escaneo mejorado, escaneo básico y escaneo básico mejorado, los escaneos previamente establecidos dejarán de estar disponibles. Tendrá que volver a configurar los escaneos. Sin embargo, si vuelve a la versión de escaneo anterior, estarán disponibles los escaneos establecidos.

- **Escaneo mejorado:** Amazon ECR se integra con Amazon Inspector para proporcionar un escaneo automatizado y continuo de sus repositorios. Las imágenes de contenedor se analizan en busca de vulnerabilidades de los paquetes de idiomas de programación y sistemas operativos. A medida que aparecen nuevas vulnerabilidades, los resultados del análisis se actualizan y Amazon Inspector emite un evento EventBridge para notificártelo. El escaneo mejorado proporciona lo siguiente:
 - El sistema operativo y los lenguajes de programación empaquetan vulnerabilidades.
 - Dos frecuencias de escaneo: escaneo pulsado y escaneo continuo.
- **Escaneo básico:** Amazon ECR ofrece dos versiones del escaneo básico que utilizan la base de datos de vulnerabilidades y exposiciones comunes (CVEs): la versión GA actual, que usa el proyecto Clair de código abierto, y una versión recientemente mejorada del escaneo básico (en versión preliminar), que usa nuestra tecnología nativa. AWS Con el escaneo básico, puede configurar los repositorios para el escaneo al insertar. También puede hacer escaneos manuales. Amazon ECR proporciona una lista de los resultados del escaneo. El escaneo básico proporciona lo siguiente:
 - Escaneos del sistema operativo.

- Dos frecuencias de escaneo: manual y escaneo pulsador.

Important

La nueva versión del escaneo básico no es compatible `imageScanFindingsSummary` con `imageScanStatus` la `DescribeImages` API. Para verlos, utilice la `DescribeImageScanFindings` API.

Filtros para elegir qué repositorios se escanean en Amazon ECR

Al configurar el escaneo de imágenes para su registro privado, puede usar filtros para elegir qué repositorios se escanearán.

Cuando se utiliza escaneo básico, puede especificar escaneo en filtros de inserción para determinar qué repositorios están configurados para realizar un escaneo de imagen cuando se inserten nuevas imágenes. Los repositorios que no coincidan con un análisis de escaneo básico en el filtro push se establecerán en la frecuencia de escaneo manual, lo que significa que para realizar un escaneo, debe activarlo manualmente.

Cuando se utiliza el escaneo mejorado, puede especificar filtros separados para escanear al insertar y escaneo continuo. Los repositorios que no coincidan con un filtro de escaneo mejorado tendrán deshabilitado el escaneo. Si utiliza la exploración mejorada y especifica filtros independientes para escanear al insertar y escaneo continuo donde varios filtros coinciden con el mismo repositorio, Amazon ECR aplica el filtro de escaneo continuo sobre el filtro de escaneo al insertar de ese repositorio.

Filtra los caracteres comodín

Cuando se especifica un filtro, un filtro sin comodín coincidirá con todos los nombres de repositorio que contengan el filtro. Un filtro con un comodín (*) coincide con cualquier nombre de repositorio en el que el comodín sustituya a cero o más caracteres del nombre del repositorio.

En la tabla siguiente se proporcionan ejemplos en los que los nombres de los repositorios se expresan en el eje horizontal y se especifican filtros de ejemplo en el eje vertical.

	prod	repo-prod	prod-repo	repo-prod-repo	prodrepo
prod	Sí	Sí	Sí	Sí	Sí
*prod	Sí	Sí	No	No	No
prod*	Sí	No	Sí	No	Sí
prod	Sí	Sí	Sí	Sí	Sí
prod*repo	No	No	Sí	No	Sí

Escanee imágenes para detectar vulnerabilidades de paquetes de lenguajes de programación y sistemas operativos en Amazon ECR

El escaneo mejorado de Amazon ECR es una integración con Amazon Inspector que proporciona análisis de vulnerabilidades para las imágenes de contenedor. Las imágenes de contenedor se analizan en busca de vulnerabilidades de los paquetes de idiomas de programación y sistemas operativos. Puede ver los hallazgos del escaneo tanto con Amazon ECR como con Amazon Inspector directamente. Para obtener información acerca de Amazon Inspector, consulte [Escaneo de imágenes de contenedores con Amazon Inspector](#) en la Guía del usuario de Amazon Inspector.

Con el escaneo mejorado, puede elegir qué repositorios están configurados para el escaneo automático y continuo y cuáles están configurados para el escaneo al insertar. Esto se hace configurando filtros de escaneo.

Consideraciones del escaneo mejorado

Tenga en cuenta lo siguiente antes de activar el escaneo mejorado de Amazon ECR.

- El uso de esta característica no implica costos adicionales por parte de Amazon ECR; sin embargo, sí se generan cargos de Amazon Inspector por el escaneado de las imágenes. Para obtener más información, consulte [Precios de Amazon Inspector](#).
- El análisis mejorado no es compatible con las siguientes regiones:
 - Medio Oriente (EAU) (me-central-1)
 - Asia-Pacífico (Hyderabad) (ap-south-2)

- Israel (Tel Aviv) (`il-central-1`)
- Asia-Pacífico (Melbourne) (`ap-southeast-4`)
- Europa (España) (`eu-south-2`)
- Amazon Inspector admite el escaneo de sistemas operativos específicos. Para obtener una lista completa, consulte [Sistemas operativos compatibles: escaneo de Amazon ECR](#) en la Guía del usuario de Amazon Inspector.
- Amazon Inspector utiliza un rol de IAM vinculado a servicios, que proporciona los permisos necesarios para ofrecer un escaneo mejorado de los repositorios. Amazon Inspector crea automáticamente el rol de IAM vinculado a servicios cuando se enciende el escaneo mejorado para su registro privado. Para obtener más información, consulte [Uso de roles vinculados a servicios de Amazon Inspector](#) en la Guía del usuario de Amazon Inspector.
- Al activar inicialmente el escaneo mejorado para su registro privado, Amazon Inspector solo reconoce las imágenes enviadas a Amazon ECR en los últimos 30 días, en función de la marca de tiempo de inserción de la imagen, o extraídas en los últimos 90 días. Las imágenes más antiguas tendrán el estado de escaneo `SCAN_ELIGIBILITY_EXPIRED`. Si desea que Amazon Inspector escanee estas imágenes, debe volver a subirlas a su repositorio.
- Todas las imágenes que se envían a Amazon ECR después de activar el escaneo mejorado se escanean continuamente durante el tiempo configurado. De forma predeterminada, la duración es de por vida. Esta configuración puede hacerse desde la consola de Amazon Inspector. Para obtener más información, consulte [Cambiar la duración mejorada del escaneo de imágenes en Amazon Inspector](#).
- Cuando el registro privado de Amazon ECR tiene encendido el escaneo mejorado, todos los repositorios que coinciden con los filtros de escaneo se analizan únicamente mediante el escaneo mejorado. Cualquier repositorio que no coincida con un filtro tendrá una frecuencia de escaneo `Off`, pero no se escaneará. No se admiten los escaneos manuales mediante escaneo mejorado. Para obtener más información, consulte [Filtros para elegir qué repositorios se escanean en Amazon ECR](#).
- Si especifica filtros independientes para escanear al insertar y escaneo continuo donde varios filtros coinciden con el mismo repositorio, Amazon ECR aplica el filtro de escaneo continuo sobre el filtro de escaneo al insertar de ese repositorio.
- Cuando se activa el escaneo mejorado, Amazon ECR envía un evento `EventBridge` cuando se cambia la frecuencia de escaneo de un repositorio. Amazon Inspector emite eventos `EventBridge` cuando se completa un escaneo inicial y cuando se crea, actualiza o cierra un hallazgo de escaneo de imágenes.

Se requieren permisos de IAM para mejorar el escaneo en Amazon ECR

El escaneo mejorado de Amazon ECR requiere un rol de IAM vinculado a servicios de Amazon Inspector y que la entidad principal de IAM que habilita y utiliza el escaneo mejorado tenga permisos para llamar a las API de Amazon Inspector necesarias para el escaneo. Amazon Inspector crea automáticamente el rol de IAM vinculado a servicios cuando se enciende el escaneo mejorado para su registro privado. Para obtener más información, consulte [Uso de roles vinculados a servicios de Amazon Inspector](#) en la Guía del usuario de Amazon Inspector.

La siguiente política de IAM concede los permisos necesarios para habilitar y utilizar el escaneo mejorado. Incluye el permiso necesario para que Amazon Inspector cree el rol de IAM vinculado a servicios, así como los permisos de la API de Amazon Inspector necesarios para encender y apagar el escaneo mejorado y recuperar los hallazgos del escaneo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "inspector2:Enable",
        "inspector2:Disable",
        "inspector2:ListFindings",
        "inspector2:ListAccountPermissions",
        "inspector2:ListCoverage"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "inspector2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

}

Configuración del escaneo mejorado de imágenes en Amazon ECR

Configure el escaneo mejorado por región para su registro privado.

Compruebe que dispone de los permisos de IAM adecuados para configurar el escaneo mejorado. Para obtener más información, consulte [Se requieren permisos de IAM para mejorar el escaneo en Amazon ECR](#).

AWS Management Console

Para activar el análisis mejorado de su registro privado

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/repositories>.
2. En la barra de navegación, elija la región para la que desea establecer la configuración de escaneo.
3. En el panel de navegación, selecciona Registro privado, Configuración y Escaneo.
4. En la página Scanning configuration (Configuración de escaneo), para Scan type (Tipo de escaneo) elija Enhanced scanning (Escaneo mejorado).

De forma predeterminada, cuando se selecciona Escaneo mejorado, todos los repositorios se escanean de forma continua.

5. Para elegir repositorios específicos para escanearlos de forma continua, desactive la casilla Escanear continuamente todos los repositorios y, a continuación, defina los filtros:

Important

Los filtros sin comodines coincidirán con todos los nombres de repositorio que contengan el filtro. Los filtros con comodines (*) coinciden con un nombre de repositorio donde el comodín reemplaza cero o más caracteres del nombre. Para ver ejemplos del comportamiento de los filtros, consulte [the section called “Filtra los caracteres comodín”](#)

- a. Introduzca un filtro basado en los nombres de los repositorios y, a continuación, seleccione Añadir filtro.
- b. Decida qué repositorios escanear cuando se inserte una imagen:

- Para escanear todos los repositorios al insertar, seleccione Escanear al insertar todos los repositorios.
 - Para elegir repositorios específicos para escanearlos de forma automática, introduce un filtro basado en los nombres de los repositorios y, a continuación, selecciona Añadir filtro.
6. Seleccione Guardar.
 7. Repita estos pasos en cada región en la que desee encender el escaneo mejorado.

AWS CLI

Utilice el siguiente AWS CLI comando para activar el análisis mejorado de su registro privado mediante el AWS CLI. Puede especificar filtros de escaneo mediante el objeto de `rules`.

- [put-registry-scanning-configuration](#) (AWS CLI)

En el ejemplo siguiente se enciende el escaneo mejorado del registro privado. De forma predeterminada, cuando no se especifican `rules`, Amazon ECR establece la configuración de escaneo en escaneo continuo para todos los repositorios.

```
aws ecr put-registry-scanning-configuration \
  --scan-type ENHANCED \
  --region us-east-2
```

El siguiente ejemplo enciende un escaneo mejorado para su registro privado y especifica un filtro de escaneo. El filtro de escaneo del ejemplo enciende el escaneo continuo de todos los repositorios con `prod` en su nombre.

```
aws ecr put-registry-scanning-configuration \
  --scan-type ENHANCED \
  --rules '[{"repositoryFilters" : [{"filter": "prod", "filterType" :  
"WILDCARD"}], "scanFrequency" : "CONTINUOUS_SCAN"}]' \
  --region us-east-2
```

El siguiente ejemplo enciende un escaneo mejorado para su registro privado y especifica varios filtros de escaneo. Los filtros de escaneo en el ejemplo enciende el escaneo continuo para todos los repositorios con `prod` en su nombre y enciende el escaneo al insertar solo para todos los demás repositorios.


```
aws ecr put-registry-scanning-configuration \  
  --scan-type ENHANCED \  
  --rules '[{"repositoryFilters" : [{"filter": "prod", "filterType" :  
  "WILDCARD"}], "scanFrequency" : "CONTINUOUS_SCAN"}, {"repositoryFilters" :  
  [{"filter": "*", "filterType" : "WILDCARD"}], "scanFrequency" : "SCAN_ON_PUSH"}]' \  
  --region us-west-2
```

Cambiar la duración mejorada del escaneo de imágenes en Amazon Inspector

Puede cambiar el número de días que Amazon Inspector escanea continuamente las imágenes de sus repositorios privados de Amazon ECR. De forma predeterminada, cuando el análisis mejorado está encendido para su registro privado de Amazon ECR, el servicio Amazon Inspector supervisa continuamente sus repositorios hasta que se elimina la imagen o se desactiva el análisis mejorado. La duración durante la que Amazon Inspector analiza sus imágenes se puede cambiar mediante la configuración de Amazon Inspector. Las duraciones de análisis disponibles son Lifetime (default) (Vida útil [predeterminado]), 180 days (180 días), y 30 days (30 días). Cuando transcurre la duración del análisis de un repositorio, el estado del análisis de `SCAN_ELIGIBILITY_EXPIRED` se muestra al enumerar las vulnerabilidades de análisis. Para obtener más información, consulte [Changing the Amazon ECR automated re-scan duration](#) (Cambiar la duración del reanálisis automático de Amazon ECR) en la Guía del usuario de Amazon Inspector.

Para cambiar la configuración de duración de análisis mejorado

1. Abra la consola de Amazon Inspector en <https://console.aws.amazon.com/inspector/v2/home>.
2. En el panel de navegación izquierdo, expanda Settings (Configuración) y, a continuación, General.
3. En la página Settings (Configuración), en ECR re-scan duration (Duración del reanálisis de ECR), elija una configuración y, a continuación, elija Save (Guardar).

EventBridge eventos enviados para un escaneo mejorado en Amazon ECR

Cuando se activa el escaneo mejorado, Amazon ECR envía un evento EventBridge cuando se cambia la frecuencia de escaneo de un repositorio. Amazon Inspector envía los eventos EventBridge cuando se completa un escaneo inicial y cuando se crea, actualiza o cierra un hallazgo de escaneo de imágenes.

Evento de cambio de frecuencia de escaneo de repositorio

Cuando el escaneo mejorado está encendido para su registro, Amazon ECR envía el siguiente evento cuando se produce un cambio con un recurso que tiene encendido el escaneo mejorado. Esto incluye la creación de nuevos repositorios, la frecuencia de escaneo de un repositorio que se está modificando o cuando se crean o eliminan imágenes en repositorios con el escaneo mejorado encendido. Para obtener más información, consulte [Escanee imágenes en busca de vulnerabilidades de software en Amazon ECR](#).

```
{
  "version": "0",
  "id": "0c18352a-a4d4-6853-ef53-0abEXAMPLE",
  "detail-type": "ECR Scan Resource Change",
  "source": "aws.ecr",
  "account": "123456789012",
  "time": "2021-10-14T20:53:46Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "action-type": "SCAN_FREQUENCY_CHANGE",
    "repositories": [{
      "repository-name": "repository-1",
      "repository-arn": "arn:aws:ecr:us-east-1:123456789012:repository/repository-1",
      "scan-frequency": "SCAN_ON_PUSH",
      "previous-scan-frequency": "MANUAL"
    },
    {
      "repository-name": "repository-2",
      "repository-arn": "arn:aws:ecr:us-east-1:123456789012:repository/repository-2",
      "scan-frequency": "CONTINUOUS_SCAN",
      "previous-scan-frequency": "SCAN_ON_PUSH"
    },
    {
      "repository-name": "repository-3",
      "repository-arn": "arn:aws:ecr:us-east-1:123456789012:repository/repository-3",
      "scan-frequency": "CONTINUOUS_SCAN",
      "previous-scan-frequency": "SCAN_ON_PUSH"
    }
  ],
  "resource-type": "REPOSITORY",
  "scan-type": "ENHANCED"
}
```

```
}
```

Evento de un escaneo de imagen inicial (escaneo mejorado)

Cuando el escaneo mejorado está encendido para el registro, Amazon Inspector envía el siguiente evento cuando finaliza el escaneo de imágenes inicial. El parámetro `finding-severity-counts` solo devolverá un valor para un nivel de gravedad, si existe. Por ejemplo, si la imagen no contiene resultados de nivel CRITICAL, no se devolverá ningún recuento crítico. Para obtener más información, consulte [Escanee imágenes para detectar vulnerabilidades de paquetes de lenguajes de programación y sistemas operativos en Amazon ECR](#).

Patrón de eventos:

```
{
  "source": ["aws.inspector2"],
  "detail-type": ["Inspector2 Scan"]
}
```

Ejemplo de salida:

```
{
  "version": "0",
  "id": "739c0d3c-4f02-85c7-5a88-94a9EXAMPLE",
  "detail-type": "Inspector2 Scan",
  "source": "aws.inspector2",
  "account": "123456789012",
  "time": "2021-12-03T18:03:16Z",
  "region": "us-east-2",
  "resources": [
    "arn:aws:ecr:us-east-2:123456789012:repository/amazon/amazon-ecs-sample"
  ],
  "detail": {
    "scan-status": "INITIAL_SCAN_COMPLETE",
    "repository-name": "arn:aws:ecr:us-east-2:123456789012:repository/amazon/amazon-ecs-sample",
    "finding-severity-counts": {
      "CRITICAL": 7,
      "HIGH": 61,
      "MEDIUM": 62,
      "TOTAL": 158
    }
  },
}
```

```

    "image-digest":
      "sha256:36c7b282abd0186e01419f2e58743e1bf635808231049bbc9d77e5EXAMPLE",
    "image-tags": [
      "latest"
    ]
  }
}

```

Evento para una actualización de búsqueda de escaneo de imagen (escaneo mejorado)

Cuando el escaneo mejorado está encendido para su registro, Amazon Inspector envía el siguiente evento cuando se crea, actualiza o cierra el hallazgo del escaneo de imágenes. Para obtener más información, consulte [Escanee imágenes para detectar vulnerabilidades de paquetes de lenguajes de programación y sistemas operativos en Amazon ECR](#).

Patrón de eventos:

```

{
  "source": ["aws.inspector2"],
  "detail-type": ["Inspector2 Finding"]
}

```

Ejemplo de salida:

```

{
  "version": "0",
  "id": "42dbea55-45ad-b2b4-87a8-afaEXAMPLE",
  "detail-type": "Inspector2 Finding",
  "source": "aws.inspector2",
  "account": "123456789012",
  "time": "2021-12-03T18:02:30Z",
  "region": "us-east-2",
  "resources": [
    "arn:aws:ecr:us-east-2:123456789012:repository/amazon/amazon-ecs-sample/sha256:36c7b282abd0186e01419f2e58743e1bf635808231049bbc9d77eEXAMPLE"
  ],
  "detail": {
    "awsAccountId": "123456789012",
    "description": "In libssh2 v1.9.0 and earlier versions, the SSH_MSG_DISCONNECT logic in packet.c has an integer overflow in a bounds check, enabling an attacker to specify an arbitrary (out-of-bounds) offset for a subsequent memory read. A crafted SSH server may be able to disclose sensitive information or cause a denial of service condition on the client system when a user connects to the server.",
  }
}

```

```
"findingArn": "arn:aws:inspector2:us-east-2:123456789012:finding/
be674aadd0f75ac632055EXAMPLE",
"firstObservedAt": "Dec 3, 2021, 6:02:30 PM",
"inspectorScore": 6.5,
"inspectorScoreDetails": {
  "adjustedCvss": {
    "adjustments": [],
    "cvssSource": "REDHAT_CVE",
    "score": 6.5,
    "scoreSource": "REDHAT_CVE",
    "scoringVector": "CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N",
    "version": "3.0"
  }
},
"lastObservedAt": "Dec 3, 2021, 6:02:30 PM",
"packageVulnerabilityDetails": {
  "cvss": [
    {
      "baseScore": 6.5,
      "scoringVector": "CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N",
      "source": "REDHAT_CVE",
      "version": "3.0"
    },
    {
      "baseScore": 5.8,
      "scoringVector": "AV:N/AC:M/Au:N/C:P/I:N/A:P",
      "source": "NVD",
      "version": "2.0"
    },
    {
      "baseScore": 8.1,
      "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H",
      "source": "NVD",
      "version": "3.1"
    }
  ],
  "referenceUrls": [
    "https://access.redhat.com/errata/RHSA-2020:3915"
  ],
  "source": "REDHAT_CVE",
  "sourceUrl": "https://access.redhat.com/security/cve/CVE-2019-17498",
  "vendorCreatedAt": "Oct 16, 2019, 12:00:00 AM",
  "vendorSeverity": "Moderate",
  "vulnerabilityId": "CVE-2019-17498",
}
```

```

    "vulnerablePackages": [
      {
        "arch": "X86_64",
        "epoch": 0,
        "name": "libssh2",
        "packageManager": "OS",
        "release": "12.amzn2.2",
        "sourceLayerHash":
"sha256:72d97abdfae3b3c933ff41e39779cc72853d7bd9dc1e4800c5294dEXAMPLE",
        "version": "1.4.3"
      }
    ],
    "remediation": {
      "recommendation": {
        "text": "Update all packages in the vulnerable packages section to
their latest versions."
      }
    },
    "resources": [
      {
        "details": {
          "awsEcrContainerImage": {
            "architecture": "amd64",
            "imageHash":
"sha256:36c7b282abd0186e01419f2e58743e1bf635808231049bbc9d77e5EXAMPLE",
            "imageTags": [
              "latest"
            ],
            "platform": "AMAZON_LINUX_2",
            "pushedAt": "Dec 3, 2021, 6:02:13 PM",
            "registry": "123456789012",
            "repositoryName": "amazon/amazon-ecs-sample"
          }
        },
        "id": "arn:aws:ecr:us-east-2:123456789012:repository/amazon/amazon-ecs-
sample/sha256:36c7b282abd0186e01419f2e58743e1bf635808231049bbc9d77EXAMPLE",
        "partition": "N/A",
        "region": "N/A",
        "type": "AWS_ECR_CONTAINER_IMAGE"
      }
    ],
    "severity": "MEDIUM",
    "status": "ACTIVE",

```

```
"title": "CVE-2019-17498 - libssh2",  
"type": "PACKAGE_VULNERABILITY",  
"updatedAt": "Dec 3, 2021, 6:02:30 PM"  
}  
}
```

Recuperación de los resultados para escaneos mejorados en Amazon ECR

Puede recuperar los resultados de la última digitalización mejorada de imágenes completada y, a continuación, abrirlas en Amazon Inspector para ver más detalles. Las vulnerabilidades de software descubiertas se enumeran por gravedad según la base de datos de vulnerabilidades y exposiciones comunes (CVE).

Para obtener detalles sobre la solución de problemas comunes al escanear imágenes, consulte [Solución de problemas de digitalización de imágenes en Amazon ECR](#).

AWS Management Console

Siga los pasos siguientes para recuperar los resultados del escaneo de imágenes mediante la AWS Management Console.

Para recuperar los resultados del escaneo de imágenes

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/repositories>.
2. En la barra de navegación, elija la Región donde se encuentra su repositorio.
3. En el panel de navegación, elija Repositories (Repositorios).
4. En la página Repositories (Repositorios) elija el repositorio que contiene la imagen para recuperar los resultados del escaneo.
5. En la página Images (Imágenes), en la columna Vulnerabilities (Vulnerabilidades), seleccione See findings (Ver resultados) de la imagen para recuperar los resultados del escaneo.
6. Para ver más detalles en la consola de Amazon Inspector, elija el nombre de la vulnerabilidad en la columna Nombre.

AWS CLI

Utilice el siguiente AWS CLI comando para recuperar los resultados del escaneo de imágenes mediante el AWS CLI. Puede especificar una imagen utilizando `imageTag` o `imageDigest`, ambos se pueden obtener mediante el comando [list-images](#) de la CLI.

- [describe-image-scan-findings](#) (AWS CLI)

En el ejemplo siguiente se utiliza una etiqueta de imagen.

```
aws ecr describe-image-scan-findings \  
  --repository-name name \  
  --image-id imageTag=tag_name \  
  --region us-east-2
```

En el ejemplo siguiente se utiliza un resumen de imágenes.

```
aws ecr describe-image-scan-findings \  
  --repository-name name \  
  --image-id imageDigest=sha256_hash \  
  --region us-east-2
```

Escanee imágenes en busca de vulnerabilidades del sistema operativo en Amazon ECR

La función de digitalización básica mejorada se encuentra en la versión preliminar de Amazon ECR y está sujeta a cambios. Durante esta versión preliminar pública, solo podrá utilizarla para suscribirse AWS Management Console a la versión de digitalización básica mejorada.

Amazon ECR ofrece dos versiones de análisis básico que utilizan la base de datos de vulnerabilidades y exposiciones comunes (CVEs):

- La versión actual de GA que utiliza el proyecto Clair de código abierto. [Para obtener más información sobre Clair, consulte Clair en GitHub](#)
- La versión recientemente mejorada del escaneo básico (en versión preliminar) que utiliza tecnología AWS nativa.

Amazon ECR utiliza la gravedad de un CVE de la fuente de distribución ascendente, si está disponible. De lo contrario, se utiliza la puntuación del Common Vulnerability Scoring System (CVSS). La puntuación CVSS se puede utilizar para obtener la calificación de gravedad de vulnerabilidad de NVD. Para obtener más información, consulte [NVD Vulnerability Severity Ratings](#).

Ambas versiones del escaneo básico de Amazon ECR admiten filtros para especificar qué repositorios se escanearán al insertarlo. Todos los repositorios que no coincidan con un filtro de escaneo automático están configurados con la frecuencia de escaneo manual, lo que significa que debe iniciar el escaneo manualmente. Se puede escanear una imagen una vez cada 24 horas. Las 24 horas incluyen el escaneo inicial instantáneo, si está configurado, y cualquier escaneo manual.

Para cada imagen se pueden recuperar los últimos resultados del escaneo de imágenes completados. Cuando se completa el escaneo de una imagen, Amazon ECR envía un evento a Amazon EventBridge. Para obtener más información, consulte [Eventos de Amazon ECR y EventBridge](#).

Soporte regional para mejorar el escaneo básico

La versión mejorada del escaneo básico es compatible con las siguientes regiones:

- Asia Pacífico (Hong Kong) (ap-east-1)
- Europa (Estocolmo) (eu-north-1)
- Medio Oriente (Baréin) (me-south-1)
- Asia-Pacífico (Bombay) (ap-south-1)
- Europa (París) (eu-west-3)
- AWS GovCloud (Este de EE. UU.) (us-gov-east-1)
- África (Ciudad del Cabo) (af-south-1)
- Asia-Pacífico (Yakarta) (ap-southeast-3)
- Europa (Fráncfort) (eu-central-1)
- Europa (Irlanda) (eu-west-1)
- América del Sur (São Paulo) (sa-east-1)
- Este de EE. UU. (Ohio) (us-east-2)
- AWS GovCloud (EEUU-Oeste) (us-gov-west-1)
- Asia-Pacífico (Tokio) (ap-northeast-1)
- Asia-Pacífico (Seúl) (ap-northeast-2)
- Asia-Pacífico (Osaka) (ap-northeast-3)
- Europa (Milán) (eu-south-1)
- Europa (Londres) (eu-west-2)
- Este de EE. UU. (Norte de Virginia) (us-east-1)

- Asia-Pacífico (Singapur) (ap-southeast-1)
- Asia-Pacífico (Sídney) (ap-southeast-2)
- Canadá (centro) (ca-central-1)
- Oeste de EE. UU. (Norte de California) (us-west-1)
- Oeste de EE. UU. (Oregón) (us-west-2)
- Europa (Zúrich) (eu-central-2)

Compatibilidad con el sistema operativo para el escaneo básico y un escaneo básico mejorado

Como práctica recomendada de seguridad y para una cobertura continua, le recomendamos que siga utilizando las versiones compatibles de un sistema operativo. De acuerdo con la política del proveedor, los sistemas operativos discontinuados ya no se actualizan con parches y, en muchos casos, ya no se publican nuevos avisos de seguridad para ellos. A esto se suma que algunos proveedores eliminan los avisos de seguridad y las detecciones de sus fuentes cuando un sistema operativo afectado alcanza el final de la compatibilidad estándar. Cuando una distribución pierde el soporte de su proveedor, es posible que Amazon ECR deje de admitir su análisis en busca de vulnerabilidades. Cualquier hallazgo que Amazon ECR genere sobre un sistema operativo discontinuado debe utilizarse únicamente con fines informativos. A continuación se enumeran los sistemas operativos y las versiones compatibles actualmente.

Sistema operativo	Versión
Alpine Linux (Alpine)	3,19
Alpine Linux (Alpine)	3.18
Alpine Linux (Alpine)	3.17
Alpine Linux (Alpine)	3.16
Amazon Linux 2 (AL2)	AL2
Amazon Linux 2023 (AL2023)	AL2023
CentOS Linux (CentOS)	7

Sistema operativo	Versión
Debian Server (Bookworm)	12
Debian Server (Bullseye)	11
Debian Server (Buster)	10
Oracle Linux (Oracle)	9
Oracle Linux (Oracle)	8
Oracle Linux (Oracle)	7
Ubuntu (lunar)	23.04
Ubuntu (Jammy)	22.04 (LTS)
Ubuntu (Focal)	20.04 (LTS)
Ubuntu (Bionic)	18.04 (ESM)
Ubuntu (Xenial)	16.04 (ESM)
Ubuntu (Trusty)	14.04 (ESM)
Red Hat Enterprise Linux (RHEL)	7
Red Hat Enterprise Linux (RHEL)	8
Red Hat Enterprise Linux (RHEL)	9

Configuración del escaneado básico mejorado de imágenes en Amazon ECR

Ya está disponible en versión preliminar una versión mejorada del escaneo básico de Amazon ECR. El escaneo básico mejorado utiliza tecnología AWS nativa.

Configure el escaneo básico mejorado por región para su repositorio privado. Para obtener una lista de las regiones que admiten un escaneo básico mejorado, consulte [Soporte regional para mejorar el escaneo básico](#).

Para activar el escaneo básico mejorado de su registro privado

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/repositories>.
2. En la barra de navegación, elija la región para la que desea establecer la configuración de escaneo.
3. En el panel de navegación, elija Private registry (Registro privado), Scanning (Escaneo).
4. En la página de configuración del escaneo, en Tipo de escaneo, elija Escaneo básico mejorado (en vista previa): nuevo.
5. De forma predeterminada, todos los repositorios están configurados para el escaneo manual. Opcionalmente, puede encender el escaneo push especificando Escaneo en filtros de inserción. Puede configurar el escaneo al insertar para todos los repositorios o para repositorios individuales. Para obtener más información, consulte [Filtros para elegir qué repositorios se escanean en Amazon ECR](#).

Configuración del escaneado básico de imágenes en Amazon ECR

De forma predeterminada, Amazon ECR activa el escaneo básico para todos los registros privados. Como resultado, a menos que haya cambiado la configuración de digitalización de su registro privado, no es necesario activar la digitalización básica. El escaneo básico utiliza el proyecto Clair de código abierto.

Puede seguir los siguientes pasos para definir uno o más escaneos con filtros push.

Para activar el escaneo básico de su registro privado

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/repositories>.
2. En la barra de navegación, elija la región para la que desea establecer la configuración de escaneo.
3. En el panel de navegación, elija Private registry (Registro privado), Scanning (Escaneo).
4. En la página Scanning configuration (Configuración de escaneo) Para Scan type (Tipo de escaneo), elija Basic scanning (Escaneo básico).

- De forma predeterminada, todos los repositorios están configurados para el escaneo manual. Opcionalmente, puede encender el escaneo push especificando Escaneo en filtros de inserción. Puede configurar el escaneo al insertar para todos los repositorios o para repositorios individuales. Para obtener más información, consulte [Filtros para elegir qué repositorios se escanean en Amazon ECR](#).

Escaneo manual de una imagen en busca de vulnerabilidades del sistema operativo en Amazon ECR

Si sus repositorios no están configurados para escanear de forma automática, puede iniciar los escaneos de imágenes manualmente. Se puede escanear una imagen una vez cada 24 horas. Las 24 horas incluyen el escaneo inicial instantáneo, si está configurado, y cualquier escaneo manual.

Para obtener detalles sobre la solución de problemas comunes al escanear imágenes, consulte [Solución de problemas de digitalización de imágenes en Amazon ECR](#).

AWS Management Console

Siga los pasos siguientes para comenzar el escaneo manual de una imagen mediante la AWS Management Console.

- Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/repositories>.
- En la barra de navegación, elija la región en la que va a crear el repositorio.
- En el panel de navegación, elija Repositories (Repositorios).
- En la página Repositories (Repositorios), elija el repositorio del que contiene la imagen que desea escanear.
- En la página Images (Imágenes) seleccione la imagen que desea escanear y, a continuación, elija Scan (Escanear).

AWS CLI

- [start-image-scan](#) (AWS CLI)

En el ejemplo siguiente se utiliza una etiqueta de imagen.

```
aws ecr start-image-scan --repository-name name --image-id imageTag=tag_name --  
region us-east-2
```

En el ejemplo siguiente se utiliza un resumen de imágenes.

```
aws ecr start-image-scan --repository-name name --image-id imageDigest=sha256_hash
--region us-east-2
```

AWS Tools for Windows PowerShell

- [Búsqueda Get-ECR \(\) ImageScan](#) AWS Tools for Windows PowerShell

En el ejemplo siguiente se utiliza una etiqueta de imagen.

```
Start-ECRImageScan -RepositoryName name -ImageId_ImageTag tag_name -Region us-
east-2 -Force
```

En el ejemplo siguiente se utiliza un resumen de imágenes.

```
Start-ECRImageScan -RepositoryName name -ImageId_ImageDigest sha256_hash -
Region us-east-2 -Force
```

Recuperación de los resultados de los escaneos básicos en Amazon ECR

Puede recuperar los resultados de la última digitalización básica de imágenes completada. Las vulnerabilidades de software descubiertas se enumeran por gravedad según la base de datos de vulnerabilidades y exposiciones comunes (CVE).

Para obtener detalles sobre la solución de problemas comunes al escanear imágenes, consulte [Solución de problemas de digitalización de imágenes en Amazon ECR](#).

AWS Management Console

Siga los pasos siguientes para recuperar los resultados del escaneo de imágenes mediante la AWS Management Console.

Para recuperar los resultados del escaneo de imágenes

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/repositories>.
2. En la barra de navegación, elija la región en la que va a crear el repositorio.

3. En el panel de navegación, elija Repositories (Repositorios).
4. En la página Repositories (Repositorios) elija el repositorio que contiene la imagen para recuperar los resultados del escaneo.
5. En la página Images (Imágenes), en la columna Vulnerabilities (Vulnerabilidades), seleccione Details (Detalles) para la imagen para la que desea recuperar los resultados del escaneo.

AWS CLI

Utilice el siguiente AWS CLI comando para recuperar los resultados del escaneo de imágenes mediante el AWS CLI. Puede especificar una imagen utilizando `imageTag` o `imageDigest`, ambos se pueden obtener mediante el comando [list-images](#) de la CLI.

- [describe-image-scan-findings](#) (AWS CLI)

En el ejemplo siguiente se utiliza una etiqueta de imagen.

```
aws ecr describe-image-scan-findings --repository-name name --image-id  
imageTag=tag_name --region us-east-2
```

En el ejemplo siguiente se utiliza un resumen de imágenes.

```
aws ecr describe-image-scan-findings --repository-name name --image-id  
imageDigest=sha256_hash --region us-east-2
```

AWS Tools for Windows PowerShell

- [Búsqueda Get-ECR \(\) ImageScan](#) AWS Tools for Windows PowerShell

En el ejemplo siguiente se utiliza una etiqueta de imagen.

```
Get-ECRImageScanFinding -RepositoryName name -ImageId_ImageTag tag_name -  
Region us-east-2
```

En el ejemplo siguiente se utiliza un resumen de imágenes.

```
Get-ECRImageScanFinding -RepositoryName name -ImageId_ImageDigest sha256_hash -  
Region us-east-2
```

Solución de problemas de digitalización de imágenes en Amazon ECR

A continuación se presentan errores comunes de escaneo de imágenes. Puede ver errores como este en la consola de Amazon ECR mostrando los detalles de la imagen o mediante la API o AWS CLI mediante la `DescribeImageScanFindings` API.

UnsupportedImageError

Puede obtener un error `UnsupportedImageError` al intentar escanear una imagen creada con un sistema operativo para el que Amazon ECR no admite el escaneo de imágenes básico. Amazon ECR admite el escaneo de vulnerabilidades de paquetes para las versiones principales de Amazon Linux, Amazon Linux 2, Debian, Ubuntu, CentOS, Oracle Linux, Alpine y distribuciones de Linux RHEL. Una vez que una distribución pierde el soporte de su proveedor, es posible que Amazon ECR ya no admita escanearla en busca de vulnerabilidades. Amazon ECR no admite el escaneo de imágenes creadas a partir de la imagen [temporal de Docker](#).

Important

Cuando se utiliza un escaneo mejorado, Amazon Inspector admite el escaneo de sistemas operativos y tipos de medios específicos. Para obtener una lista completa, consulte [Sistemas operativos compatibles y tipos de medios](#) en la Guía del usuario de Amazon Inspector.

Se devuelve un nivel de gravedad UNDEFINED

Es posible que reciba un resultado de escaneo que tenga un nivel de gravedad de UNDEFINED. Las siguientes son las causas comunes para esto:

- El origen de CVE no asignó prioridad a la vulnerabilidad.
- A la vulnerabilidad se le asignó una prioridad que Amazon ECR no reconocía.

Para determinar la gravedad y la descripción de una vulnerabilidad, puede ver las CVE directamente desde el origen.

Descripción del estado de análisis **SCAN_ELIGIBILITY_EXPIRED**

Cuando el análisis mejorado con Amazon Inspector está habilitado para su registro privado y está viendo sus vulnerabilidades de análisis, es posible que vea un estado de análisis de `SCAN_ELIGIBILITY_EXPIRED`. Estas pueden ser algunas de las causas:

- Al activar por primera vez el escaneo mejorado para su registro privado, Amazon Inspector solo reconoce las imágenes enviadas a Amazon ECR en los últimos 30 días, según la marca de tiempo de envío de las imágenes. Las imágenes más antiguas tendrán el estado de escaneo `SCAN_ELIGIBILITY_EXPIRED`. Si desea que Amazon Inspector escanee estas imágenes, debe volver a subirlas a su repositorio.
- Si el archivo de duración del reanálisis de ECR se cambia en la consola de Amazon Inspector y transcurre ese tiempo, el estado de análisis de la imagen cambia a `inactive` con un código de motivo de `expired`, y se programa el cierre de todos los hallazgos asociados a la imagen. Esto hace que la consola de Amazon ECR muestre el estado del análisis como `SCAN_ELIGIBILITY_EXPIRED`.

Sincronice un registro anterior con un registro privado de Amazon ECR

Mediante las reglas de extracción de caché, puede sincronizar el contenido de un registro anterior con su registro privado de Amazon ECR.

Amazon ECR permite actualmente crear reglas de caché de extracción para los siguientes registros de extracción.

- Docker Hub, Microsoft Azure Container Registry, GitHub Container Registry y GitLab Container Registry (requiere autenticación)
- Amazon ECR Public, el registro de imágenes de contenedores de Kubernetes y Quay (no requiere autenticación)

En el GitLab caso de Container Registry, Amazon ECR solo admite la extracción de caché con GitLab software-as-a-service offer, GitLab .com.

En el caso de los registros originales que requieren autenticación, debe almacenar sus credenciales en secreto. AWS Secrets Manager La consola Amazon ECR le facilita la creación del secreto de Secrets Manager para cada uno de los registros ascendentes autenticados. Para obtener más información sobre la creación de un secreto de Secrets Manager mediante la consola de Secrets Manager, consulte [Almacenar en secreto las credenciales del repositorio principal AWS Secrets Manager](#).

Después de crear una regla de caché de extracción para el registro principal, simplemente extraiga una imagen de ese registro anterior mediante el URI de su registro privado de Amazon ECR. A continuación, Amazon ECR crea un repositorio y guarda en caché la imagen en su registro privado. En las solicitudes de extracción posteriores de la imagen almacenada en caché con una etiqueta determinada, Amazon ECR comprueba el registro principal para ver si hay una nueva versión de la imagen con esa etiqueta específica e intenta actualizar la imagen en su registro privado al menos una vez cada 24 horas.

Plantillas de creación de repositorios

Amazon ECR ha agregado soporte para las plantillas de creación de repositorios, actualmente en versión preliminar, lo que le permite especificar las configuraciones iniciales de los nuevos

repositorios creados por Amazon ECR en su nombre mediante reglas de caché de extracción. Cada plantilla contiene un prefijo de espacio de nombres de repositorio que se utiliza para hacer coincidir los nuevos repositorios con una plantilla específica. Las plantillas pueden especificar la configuración de todos los ajustes del repositorio, incluidas las políticas de acceso basadas en los recursos, la inmutabilidad de las etiquetas, el cifrado y las políticas de ciclo de vida. La configuración de una plantilla de creación de repositorios solo se aplica durante la creación del repositorio y no tiene ningún efecto en los repositorios existentes ni en los repositorios creados mediante cualquier otro método. Para obtener más información, consulte [Plantillas para controlar los repositorios creados durante una acción de extracción de caché](#).

Consideraciones sobre el uso de las reglas de extracción de caché

Tenga en cuenta lo siguiente cuando utilice las reglas de extracción de caché de Amazon ECR.

- La creación de reglas de caché de extracción no se admite en las siguientes regiones.
 - China (Pekín) (cn-north-1)
 - China (Ningxia) (cn-northwest-1)
 - AWS GovCloud (Este de EE. UU.) () us-gov-east-1
 - AWS GovCloud (EEUU-Oeste) () us-gov-west-1
- AWS Lambda no admite la extracción de imágenes de contenedores de Amazon ECR mediante una regla de extracción de caché.
- Al extraer imágenes mediante caché de extracción, los puntos de conexión de servicio de FIPS de Amazon ECR no se admiten la primera vez que se extrae una imagen. Sin embargo, el uso de los puntos de conexión de servicio de FIPS de Amazon ECR funciona en extracciones posteriores.
- Cuando se extrae una imagen en caché a través del URI del registro privado de Amazon ECR, las extracciones de imágenes se inician mediante AWS direcciones IP. Esto garantiza que la extracción de imágenes no se tenga en cuenta en ninguna cuota de tasa de extracción implementada por el registro ascendente.
- Cuando una imagen almacenada en caché se extrae a través del URI del registro privado de Amazon ECR, Amazon ECR comprueba el repositorio ascendente al menos una vez cada 24 horas para verificar si la imagen almacenada en caché es la última versión. Si hay una imagen más reciente en el registro original, Amazon ECR intenta actualizar la imagen en caché. Este temporizador se basa en la última extracción de la imagen almacenada en caché.
- Si Amazon ECR no puede actualizar la imagen desde el registro original por algún motivo y se extrae la imagen, se seguirá extrayendo la última imagen en caché.

- Al crear el secreto de Secrets Manager que contiene las credenciales de registro anteriores, el nombre del secreto debe usar el `ecr-pullthroughcache/` prefijo. El secreto también debe estar en la misma cuenta y región en las que se creó la regla de caché de extracción.
- Cuando se extrae una imagen multiarquitectura mediante una regla de caché de extracción, la lista de manifiestos y cada imagen a la que se hace referencia en la lista de manifiestos se extraen al repositorio de Amazon ECR. Si solo desea extraer una arquitectura específica, puede extraer la imagen mediante el resumen de imagen o la etiqueta asociada a la arquitectura en lugar de la etiqueta asociada a la lista de manifiestos.
- Amazon ECR utiliza un rol de IAM vinculada al servicio, que proporciona los permisos necesarios para que Amazon ECR cree el repositorio, recupere el valor secreto de Secrets Manager para la autenticación y envíe la imagen almacenada en caché en su nombre. El rol de IAM vinculado a servicios se crea automáticamente cuando se crea una regla de caché de extracción. Para obtener más información, consulte [Rol vinculado a servicios de Amazon ECR para la caché de extracción](#).
- De forma predeterminada, la entidad principal de IAM que extrae la imagen almacenada en caché tiene los permisos otorgados a través de su política de IAM. Puede utilizar la política de permisos de registro privado de Amazon ECR para ampliar los permisos de una entidad de IAM. Para obtener más información, consulte [Uso de permisos de registro](#).
- Los repositorios de Amazon ECR creados mediante el flujo de trabajo de caché de extracción se tratan como cualquier otro repositorio de Amazon ECR. Se admiten todas las características del repositorio, como la replicación y el escaneo de imágenes.
- Cuando Amazon ECR crea un repositorio nuevo en su nombre mediante una acción de caché de extracción, se aplican las siguientes configuraciones predeterminadas al repositorio, a menos que haya una plantilla de creación de repositorios coincidente. Puede utilizar una plantilla de creación de repositorios para definir la configuración que se aplicará a los repositorios creados por Amazon ECR en su nombre. Para obtener más información, consulte [Plantillas para controlar los repositorios creados durante una acción de extracción de caché](#).
 - Inmutabilidad de las etiquetas: si están desactivadas, las etiquetas son mutables y se pueden sobrescribir.
 - Cifrado: se usa el cifrado predeterminado AES256.
 - Permisos de repositorio: omitidos, no se aplica ninguna política de permisos de repositorio.
 - Política de ciclo de vida: si se omite, no se aplica ninguna política de ciclo de vida.
 - Etiquetas de recursos: se omiten, no se aplica ninguna etiqueta de recursos.

- Al activar la inmutabilidad de las etiquetas de imagen en los repositorios mediante una regla de caché de extracción impedirá que Amazon ECR actualice las imágenes que utilicen la misma etiqueta.
- Cuando se extrae una imagen utilizando la regla de extracción de memoria caché por primera vez, es posible que se requiera una ruta a Internet. Hay ciertas circunstancias en las que se requiere una ruta a Internet, por lo que es mejor configurar una ruta para evitar cualquier fallo. Por lo tanto, si ha configurado Amazon ECR para que utilice una interfaz que AWS PrivateLink utilice un punto de enlace de VPC, debe asegurarse de que la primera extracción tenga una ruta a Internet. Una forma de hacerlo es crear una subred pública en la misma VPC, con una puerta de enlace a Internet, y luego enrutar todo el tráfico saliente a Internet desde su subred privada a la subred pública. La posterior extracción de imágenes mediante la regla de extracción de memoria caché no requiere esta opción. Para obtener más información, consulte [Opciones de enrutamiento](#) de ejemplo en la guía de usuarios de Amazon Virtual Private Cloud.

Se requieren permisos de IAM para sincronizar un registro ascendente con un registro privado de Amazon ECR

Además de los permisos de la API de Amazon ECR necesarios para autenticarse en un registro privado y para insertar y extraer imágenes, se necesitan los siguientes permisos adicionales para utilizar reglas de caché de extracción.

- `ecr:CreatePullThroughCacheRule`: otorga permiso para crear una regla de caché de extracción. Este permiso debe otorgarse a través de una política de IAM basada en identidad.
- `ecr:BatchImportUpstreamImage`: otorga permiso para recuperar la imagen externa e importarla a su registro privado. Este permiso se puede otorgar utilizando la política de permisos de registro privado, una política de IAM basada en identidad o mediante la política de permisos de repositorio basada en recursos. Para obtener más información sobre el uso de permisos de repositorio, consulte [Políticas de repositorios privados en Amazon ECR](#).
- `ecr:CreateRepository`: otorga permiso para crear un repositorio en un registro privado. Este permiso es necesario si el repositorio donde se conservan las imágenes almacenadas en caché no existe todavía. Este permiso se puede otorgar mediante una política de IAM basada en identidad o bien mediante la política de permisos de registro privado.
- `ecr:TagResource`: concede permiso para agregar etiquetas de metadatos a un recurso de Amazon ECR. Este permiso solo es necesario si va a extraer una imagen que utilice una regla de caché de extracción que tenga asociada una plantilla de creación de repositorios configurada para

agregar etiquetas de recursos al repositorio. Este permiso debe otorgarse a través de una política de IAM basada en identidad.

Uso de permisos de registro

Los permisos de registro privado de Amazon ECR se pueden utilizar para abarcar los permisos de entidades de IAM individuales a fin de utilizar caché de extracción. Si una entidad de IAM tiene más permisos otorgados por una política de IAM de los que la política de permisos de registro concede, prevalece la política de IAM. Por ejemplo, si un usuario tiene concedidos permisos de `ecr:*`, no se necesitan permisos adicionales en el nivel del registro.

Para crear una política de permisos de registro privado (AWS Management Console):

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/>.
2. En la barra de navegación, elija la región en la que configurar su declaración de permisos de registro privado.
3. En el panel de navegación, elija Private registry (Registro privado), Registry permissions (Permisos de registro).
4. En la página Registry permissions (Permisos de registro), elija Generate statement (Generar declaración) .
5. Para cada declaración de política de permisos de caché de extracción que desee crear, haga lo siguiente.
 - a. Para Policy type (Tipo de política), elija Pull through cache policy (Política de caché de extracción).
 - b. Para Statement id (ID de declaración), proporcione un nombre para la política de declaración de caché de extracción.
 - c. Para AM entities (Entidades de IAM), especifique los usuarios, grupos o roles que se deben incluir en la política.
 - d. Para Repository namespace (Espacio de nombres de repositorio), seleccione la regla de caché de extracción a la que asociar la política.
 - e. Para Repository names (Nombres de repositorio), especifique el nombre base del repositorio para el que se va a aplicar la regla. Por ejemplo, si desea especificar el repositorio de Amazon Linux en Amazon ECR Public, el nombre del repositorio sería `amazonlinux`.

Para crear una política de permisos de registro privado (AWS CLI):

Utilice el siguiente AWS CLI comando para especificar los permisos de registro privado mediante el AWS CLI

1. Cree un archivo local denominado `ptc-registry-policy.json` con el contenido de la política de registro. En el siguiente ejemplo se concede el permiso `ecr-pull-through-cache-user` para crear un repositorio y extraer una imagen de la galería pública de Amazon ECR, que es el origen ascendente asociado a la regla de caché de extracción creada previamente.

```
{
  "Sid": "PullThroughCacheFromReadOnlyRole",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/ecr-pull-through-cache-user"
  },
  "Action": [
    "ecr:CreateRepository",
    "ecr:BatchImportUpstreamImage"
  ],
  "Resource": "arn:aws:ecr:us-east-1:111122223333:repository/ecr-public/*"
}
```

Important

El permiso `ecr:CreateRepository` solo es necesario si el repositorio donde se conservan las imágenes almacenadas en caché no existe todavía. Por ejemplo, si la acción de creación del repositorio y las acciones de extracción de imágenes las realizan entidades principales de IAM independientes, como un administrador y un desarrollador.

2. Utilice el comando [put-registry-policy](#) para establecer la política de registro.

```
aws ecr put-registry-policy \
  --policy-text file://ptc-registry.policy.json
```

Siguientes pasos

Una vez que esté listo para empezar a utilizar las reglas de caché de extracción, siga estos pasos.

- Crear una regla de caché de extracción. Para obtener más información, consulte [Creación de una regla de extracción de caché en Amazon ECR](#).
- Cree una plantilla de creación de repositorios. Puede utilizar una plantilla de creación de repositorios para definir la configuración que se aplicará a los repositorios creados por Amazon ECR en su nombre durante una acción de caché de extracción. Para obtener más información, consulte [Plantillas para controlar los repositorios creados durante una acción de extracción de caché](#).

Creación de una regla de extracción de caché en Amazon ECR

Para cada registro ascendente que contenga imágenes que desee almacenar en caché en su registro privado de Amazon ECR, debe crear una regla de extracción de caché.

En el caso de los registros anteriores que requieren autenticación, debe almacenar las credenciales en un secreto de Secrets Manager. Puede usar un secreto existente de o crear uno nuevo. Puede crear el secreto de Secrets Manager en la consola Amazon ECR o en la consola Secrets Manager. Para crear un secreto de Secrets Manager mediante la consola Secrets Manager en lugar de la consola Amazon ECR, consulte [Almacenar en secreto las credenciales del repositorio principal AWS Secrets Manager](#).

Requisitos previos

- Compruebe que dispone de los permisos de IAM adecuados para crear reglas de extracción de caché. Para obtener más información, consulte [Se requieren permisos de IAM para sincronizar un registro ascendente con un registro privado de Amazon ECR](#).
- Para los registros anteriores que requieren autenticación: si desea utilizar un secreto existente, compruebe que el secreto de Secrets Manager cumpla los siguientes requisitos:
 - El nombre del secreto comienza por. `ecr-pullthroughcache/` AWS Management Console Solo muestra los secretos de Secrets Manager con el `ecr-pullthroughcache/` prefijo.
 - La cuenta y la región en las que se encuentra el secreto deben coincidir con la cuenta y la región en las que se encuentra la regla de extracción de memoria caché.

Para crear una regla de caché de extracción (AWS Management Console)

Los siguientes pasos muestran cómo crear una regla de caché de extracción y un secreto de Secrets Manager mediante la consola de Amazon ECR. Para crear un secreto mediante la consola Secrets

Manager, consulte [Almacenar en secreto las credenciales del repositorio principal AWS Secrets Manager](#).

Para Amazon ECR Public, Kubernetes Container Registry o Quay


1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/>.
2. Desde la barra de navegación, elija la región en la que desea configurar su registro privado.
3. En el panel de navegación, elija Private registry (Registro privado), Pull through cache (Caché de extracción).
4. En la página Pull through cache configuration (Configuración de caché de extracción), elija Add rule (Agregar regla).
5. En la página del Paso 1: Especificar un origen, en Registro, elija Amazon ECR Public, Kubernetes o Quay de la lista de registros principales y, a continuación, elija Siguiente.
6. En la página del Paso 2: Especificar un destino, en Prefijo del repositorio de Amazon ECR, especifique el prefijo del espacio de nombres del repositorio que se utilizará al almacenar en caché las imágenes extraídas del registro público de origen y, a continuación, seleccione Siguiente. De forma predeterminada, se rellena un espacio de nombres pero también se puede especificar un espacio de nombres personalizado.
7. En la página del Paso 3: Revisar y crear, revise la configuración de la regla de caché de extracción y, a continuación, seleccione Crear.
8. Repita el paso anterior para cada caché de extracción que desee crear. Las reglas de caché de extracción se crean por separado para cada región.

Para Docker Hub

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/>.
2. Desde la barra de navegación, elija la región en la que desea configurar su registro privado.
3. En el panel de navegación, elija Private registry (Registro privado), Pull through cache (Caché de extracción).
4. En la página Pull through cache configuration (Configuración de caché de extracción), elija Add rule (Agregar regla).
5. En la página del Paso 1: Especificar un origen, en Registro, elija Docker Hub, Siguiente.
6. En la página del Paso 2: Configurar la autenticación, en Credenciales principales, debe almacenar las credenciales de autenticación de Docker Hub en un secreto de AWS Secrets

Manager . Puede especificar un secreto existente o utilizar la consola Amazon ECR para crear uno nuevo.

- a. Para usar un secreto existente, selecciona Usar un AWS secreto existente. En Nombre secreto, usa el menú desplegable para seleccionar tu secreto existente y, a continuación, selecciona Siguiente.

 Note

AWS Management Console Solo muestra los secretos de Secrets Manager con nombres que usan el `ecr-pullthroughcache/` prefijo. El secreto también debe estar en la misma cuenta y región en las que se creó la regla de caché de extracción.

- b. Para crear un secreto nuevo, selecciona Crear un AWS secreto, haz lo siguiente y, a continuación, selecciona Siguiente.
 - i. En Nombre secreto, especifique un nombre descriptivo para el secreto. Los nombres de los secretos deben contener de 1 a 512 caracteres Unicode.
 - ii. En el nombre de usuario de Docker Hub, especifique su nombre de usuario de Docker Hub.
 - iii. Para el token de acceso a Docker Hub, especifique su token de acceso a Docker Hub. Para obtener más información sobre cómo crear un token de acceso de Docker Hub, consulta [Crear y administrar los tokens de acceso](#) en la documentación de Docker.
7. En la página del Paso 3: Especificar un destino, para Prefijo del repositorio de Amazon ECR, especifique el prefijo del espacio de nombres del repositorio que se utilizará al almacenar en caché las imágenes extraídas del registro público de origen y, a continuación, seleccione Siguiente.

De forma predeterminada, se rellena un espacio de nombres pero también se puede especificar un espacio de nombres personalizado.

8. En la página del Paso 4: Revisar y crear, revise la configuración de la regla de caché de extracción y, a continuación, seleccione Crear.
9. Repita el paso anterior para cada caché de extracción que desee crear. Las reglas de caché de extracción se crean por separado para cada región.

Para GitHub Container Registry

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/>.
2. Desde la barra de navegación, elija la región en la que desea configurar su registro privado.
3. En el panel de navegación, elija Private registry (Registro privado), Pull through cache (Caché de extracción).
4. En la página Pull through cache configuration (Configuración de caché de extracción), elija Add rule (Agregar regla).
5. En el paso 1: especifique una página de origen, en Registro, elija GitHub Container Registry, Siguiente.
6. En la página Paso 2: Configurar la autenticación, en el caso de las credenciales de Upstream, debe guardar en AWS Secrets Manager secreto las credenciales de autenticación de GitHub Container Registry. Puede especificar un secreto existente o utilizar la consola Amazon ECR para crear uno nuevo.
 - a. Para usar un secreto existente, selecciona Usar un AWS secreto existente. En Nombre secreto, usa el menú desplegable para seleccionar tu secreto existente y, a continuación, selecciona Siguiente.

Note

AWS Management Console Solo muestra los secretos de Secrets Manager con nombres que usan el `ecr-pullthroughcache/` prefijo. El secreto también debe estar en la misma cuenta y región en las que se creó la regla de caché de extracción.

- b. Para crear un secreto nuevo, selecciona Crear un AWS secreto, haz lo siguiente y, a continuación, selecciona Siguiente.
 - i. En Nombre secreto, especifique un nombre descriptivo para el secreto. Los nombres de los secretos deben contener de 1 a 512 caracteres Unicode.
 - ii. Como nombre de usuario de GitHub Container Registry, especifique su nombre de usuario de GitHub Container Registry.
 - iii. Para el token de acceso a GitHub Container Registry, especifique su token de acceso a GitHub Container Registry. Para obtener más información sobre cómo crear un token de GitHub acceso, consulta [Administrar tus tokens de acceso personales](#) en la GitHub documentación.

7. En la página del Paso 3: Especificar un destino, para Prefijo del repositorio de Amazon ECR, especifique el prefijo del espacio de nombres del repositorio que se utilizará al almacenar en caché las imágenes extraídas del registro público de origen y, a continuación, seleccione Siguiente.

De forma predeterminada, se rellena un espacio de nombres pero también se puede especificar un espacio de nombres personalizado.

8. En la página del Paso 4: Revisar y crear, revise la configuración de la regla de caché de extracción y, a continuación, seleccione Crear.
9. Repita el paso anterior para cada caché de extracción que desee crear. Las reglas de caché de extracción se crean por separado para cada región.

Para Microsoft Azure Container Registry


1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/>.
2. Desde la barra de navegación, elija la región en la que desea configurar su registro privado.
3. En el panel de navegación, elija Private registry (Registro privado), Pull through cache (Caché de extracción).
4. En la página Pull through cache configuration (Configuración de caché de extracción), elija Add rule (Agregar regla).
5. En la página del Paso 1: Especificar un origen, haga lo siguiente.
 - a. Para Registry, elija Microsoft Azure Container Registry
 - b. En URL del registro de origen, especifique el nombre de Microsoft Azure Container Registry y, a continuación, elija Siguiente.

Important

Solo necesita especificar el prefijo, ya que el `.azurecr.io` sufijo se rellena en su nombre.

6. En la página del Paso 2: Configurar la autenticación, en Credenciales principales, debe almacenar las credenciales de autenticación de Microsoft Azure Container Registry en un secreto de AWS Secrets Manager. Puede especificar un secreto existente o utilizar la consola Amazon ECR para crear uno nuevo.

- a. Para usar un secreto existente, selecciona Usar un AWS secreto existente. En Nombre secreto, usa el menú desplegable para seleccionar tu secreto existente y, a continuación, selecciona Siguiente.

 Note

AWS Management Console Solo muestra los secretos de Secrets Manager con nombres que usan el `ecr-pullthroughcache/` prefijo. El secreto también debe estar en la misma cuenta y región en las que se creó la regla de caché de extracción.

- b. Para crear un secreto nuevo, selecciona Crear un AWS secreto, haz lo siguiente y, a continuación, selecciona Siguiente.
 - i. En Nombre secreto, especifique un nombre descriptivo para el secreto. Los nombres de los secretos deben contener de 1 a 512 caracteres Unicode.
 - ii. Para el nombre de usuario de Microsoft Azure Container Registry, especifique su nombre de usuario de Microsoft Azure Container Registry.
 - iii. Para el nombre de usuario de Microsoft Azure Container Registry, especifique su nombre de usuario de Microsoft Azure Container Registry. Para obtener más información sobre la creación de un token de acceso a Microsoft Azure Container Registry, consulte [Crear token: portal](#) en la documentación de Microsoft Azure.
7. En la página del Paso 3: Especificar un destino, para Prefijo del repositorio de Amazon ECR, especifique el prefijo del espacio de nombres del repositorio que se utilizará al almacenar en caché las imágenes extraídas del registro público de origen y, a continuación, seleccione Siguiente.

De forma predeterminada, se rellena un espacio de nombres pero también se puede especificar un espacio de nombres personalizado.

8. En la página del Paso 4: Revisar y crear, revise la configuración de la regla de caché de extracción y, a continuación, seleccione Crear.
9. Repita el paso anterior para cada caché de extracción que desee crear. Las reglas de caché de extracción se crean por separado para cada región.

Para GitLab Container Registry

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/>.
2. Desde la barra de navegación, elija la región en la que desea configurar su registro privado.
3. En el panel de navegación, elija Private registry (Registro privado), Pull through cache (Caché de extracción).
4. En la página Pull through cache configuration (Configuración de caché de extracción), elija Add rule (Agregar regla).
5. En el paso 1: especifique una página de origen, en Registro, elija GitLab Container Registry, Siguiente.
6. En la página Paso 2: Configurar la autenticación, en el caso de las credenciales de Upstream, debe guardar en AWS Secrets Manager secreto las credenciales de autenticación de GitLab Container Registry. Puede especificar un secreto existente o utilizar la consola Amazon ECR para crear uno nuevo.
 - a. Para usar un secreto existente, selecciona Usar un AWS secreto existente. En Nombre secreto, usa el menú desplegable para seleccionar tu secreto existente y, a continuación, selecciona Siguiente. Para obtener más información sobre la creación de un secreto de Secrets Manager mediante la consola de Secrets Manager, consulte [Almacenar en secreto las credenciales del repositorio principal AWS Secrets Manager](#).
 - b. Para crear un secreto nuevo, selecciona Crear un AWS secreto, haz lo siguiente y, a continuación, selecciona Siguiente.
 - i. En Nombre secreto, especifique un nombre descriptivo para el secreto. Los nombres de los secretos deben contener de 1 a 512 caracteres Unicode.
 - ii. Como nombre de usuario de GitLab Container Registry, especifique su nombre de usuario de GitLab Container Registry.
 - iii. Para el token de acceso a GitLab Container Registry, especifique su token de acceso a GitLab Container Registry. Para obtener más información sobre cómo crear un token de

Note

AWS Management Console Solo muestra los secretos de Secrets Manager con nombres que usan el `ecr-pullthroughcache/` prefijo. El secreto también debe estar en la misma cuenta y región en las que se creó la regla de caché de extracción.

acceso a GitLab Container Registry, consulta los [tokens de acceso personal](#), los [tokens de acceso grupal](#) o los [tokens de acceso a proyectos](#) en la GitLab documentación.

7. En la página del Paso 3: Especificar un destino, para Prefijo del repositorio de Amazon ECR, especifique el prefijo del espacio de nombres del repositorio que se utilizará al almacenar en caché las imágenes extraídas del registro público de origen y, a continuación, seleccione Siguiente.

De forma predeterminada, se rellena un espacio de nombres pero también se puede especificar un espacio de nombres personalizado.

8. En la página del Paso 4: Revisar y crear, revise la configuración de la regla de caché de extracción y, a continuación, seleccione Crear.
9. Repita el paso anterior para cada caché de extracción que desee crear. Las reglas de caché de extracción se crean por separado para cada región.

Para crear una regla de caché de extracción (AWS CLI)

Utilice el AWS CLI comando [create-pull-through-cache-rule para crear una regla](#) de extracción de caché para un registro privado de Amazon ECR. En el caso de los registros originales que requieren autenticación, debe almacenar las credenciales en un secreto de Secrets Manager. Para crear un secreto mediante la consola Secrets Manager, consulte [Almacenar en secreto las credenciales del repositorio principal AWS Secrets Manager](#).

Se proporcionan los siguientes ejemplos para cada registro ascendente compatible.

Para Amazon ECR Public

En el siguiente ejemplo se crea una regla de caché de extracción para el registro público de Amazon ECR. Especifica un prefijo de repositorio `ecr-public`, lo que da como resultado que cada repositorio se cree mediante la regla de caché de extracción para tener el esquema de nomenclatura de `ecr-public/upstream-repository-name`.

```
aws ecr create-pull-through-cache-rule \  
  --ecr-repository-prefix ecr-public \  
  --upstream-registry-url public.ecr.aws \  
  --region us-east-2
```

Para el registro de contenedores de Kubernetes

En el siguiente ejemplo se crea una regla de extracción de caché para el registro público de Kubernetes. Especifica un prefijo de repositorio `kubernetes`, lo que da como resultado que cada repositorio se cree mediante la regla de caché de extracción para tener el esquema de nomenclatura de `kubernetes/upstream-repository-name`.

```
aws ecr create-pull-through-cache-rule \  
  --ecr-repository-prefix kubernetes \  
  --upstream-registry-url registry.k8s.io \  
  --region us-east-2
```

Para Quay

El siguiente ejemplo crea una regla de extracción de caché para el registro público de Quay. Especifica un prefijo de repositorio `quay`, lo que da como resultado que cada repositorio se cree mediante la regla de caché de extracción para tener el esquema de nomenclatura de `quay/upstream-repository-name`.

```
aws ecr create-pull-through-cache-rule \  
  --ecr-repository-prefix quay \  
  --upstream-registry-url quay.io \  
  --region us-east-2
```

Para Docker Hub

El siguiente ejemplo crea una regla de caché de extracción para el registro de Docker Hub. Especifica un prefijo de repositorio `docker-hub`, lo que da como resultado que cada repositorio se cree mediante la regla de caché de extracción para tener el esquema de nomenclatura de `docker-hub/upstream-repository-name`. Debe especificar el nombre de recurso de Amazon (ARN) completo del secreto que contiene las credenciales de Docker Hub.

```
aws ecr create-pull-through-cache-rule \  
  --ecr-repository-prefix docker-hub \  
  --upstream-registry-url registry-1.docker.io \  
  --credential-arn arn:aws:secretsmanager:us-east-2:111122223333:secret:ecr-  
pullthroughcache/example1234 \  
  --region us-east-2
```


Para GitHub Container Registry

En el siguiente ejemplo, se crea una regla de extracción de caché para el GitHub Container Registry. Especifica un prefijo de repositorio `docker-hub`, lo que da como resultado que cada repositorio se cree mediante la regla de caché de extracción para tener el esquema de nomenclatura de `github/upstream-repository-name`. Debe especificar el nombre de recurso de Amazon (ARN) completo del secreto que contiene sus credenciales de GitHub Container Registry.

```
aws ecr create-pull-through-cache-rule \  
  --ecr-repository-prefix github \  
  --upstream-registry-url ghcr.io \  
  --credential-arn arn:aws:secretsmanager:us-east-2:111122223333:secret:ecr-  
pullthroughcache/example1234 \  
  --region us-east-2
```

Para Microsoft Azure Container Registry

En el siguiente ejemplo, se crea una regla de extracción de caché para Microsoft Azure Container Registry. Especifica un prefijo de repositorio `azure`, lo que da como resultado que cada repositorio se cree mediante la regla de caché de extracción para tener el esquema de nomenclatura de `azure/upstream-repository-name`. Debe especificar el nombre de recurso de Amazon (ARN) completo del secreto que contiene las credenciales de Microsoft Azure Container Registry.

```
aws ecr create-pull-through-cache-rule \  
  --ecr-repository-prefix azure \  
  --upstream-registry-url myregistry.azurecr.io \  
  --credential-arn arn:aws:secretsmanager:us-east-2:111122223333:secret:ecr-  
pullthroughcache/example1234 \  
  --region us-east-2
```

Para GitLab Container Registry

En el siguiente ejemplo, se crea una regla de extracción de caché para el GitLab Container Registry. Especifica un prefijo de repositorio `gitlab`, lo que da como resultado que cada repositorio se cree mediante la regla de caché de extracción para tener el esquema de nomenclatura de `gitlab/upstream-repository-name`. Debe especificar el nombre de recurso de Amazon (ARN) completo del secreto que contiene sus credenciales de GitLab Container Registry.

```
aws ecr create-pull-through-cache-rule \  
  --ecr-repository-prefix gitlab \  
  --region us-east-2
```

```
--upstream-registry-url registry.gitlab.com \  
--credential-arn arn:aws:secretsmanager:us-east-2:111122223333:secret:ecr-  
pullthroughcache/example1234 \  
--region us-east-2
```

Siguientes pasos

Tras crear las reglas de caché de extracción, los siguientes pasos son los siguientes:

- Cree una plantilla de creación de repositorios. Puede utilizar una plantilla de creación de repositorios para definir la configuración que se aplicará a los repositorios creados por Amazon ECR en su nombre durante una acción de caché de extracción. Para obtener más información, consulte [Plantillas para controlar los repositorios creados durante una acción de extracción de caché](#).
- Valide sus reglas de caché de extracción. Al validar una regla de caché de extracción, Amazon ECR establece una conexión de red con el registro principal, comprueba que puede acceder al secreto de Secrets Manager que contiene las credenciales del registro ascendente y que la autenticación se ha realizado correctamente. Para obtener más información, consulte [Validación de las reglas de extracción de caché en Amazon ECR](#).
- Comience a usar sus reglas de caché de extracción. Para obtener más información, consulte [Extracción de una imagen con una regla de extracción de caché en Amazon ECR](#).

Plantillas para controlar los repositorios creados durante una acción de extracción de caché

La característica de plantilla de creación de repositorio está en versión preliminar para Amazon ECR y está sujeta a cambios. Durante esta vista previa pública, solo AWS Management Console podrá utilizar las plantillas de creación de repositorios para administrar las plantillas de creación de repositorios.

Utilice las plantillas de creación de repositorios de Amazon ECR para definir la configuración de los repositorios creados por Amazon ECR en su nombre durante una acción de extracción de la memoria caché. La configuración de una plantilla de creación de repositorios solo se aplica durante la creación del repositorio y no tiene ningún efecto en los repositorios existentes ni en los repositorios creados mediante cualquier otro método.

Las plantillas de creación de repositorios no se admiten en las siguientes regiones:

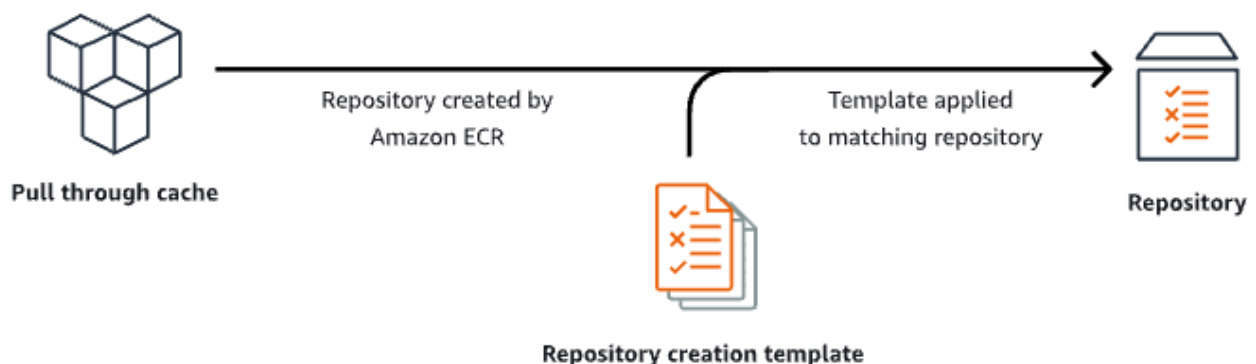
- China (Pekín) (cn-north-1)
- China (Ningxia) (cn-northwest-1)
- AWS GovCloud (Este de EE. UU.) (us-gov-east-1)
- AWS GovCloud (EEUU-Oeste) (us-gov-west-1)

Cómo funcionan las plantillas de creación de repositorios

Hay ocasiones en las que Amazon ECR necesita crear un nuevo repositorio privado en su nombre. Por ejemplo, la primera vez que utilice una regla de caché de extracción para recuperar el contenido de un repositorio de origen y almacenarlo en su registro privado de Amazon ECR. Cuando no hay una plantilla de creación de repositorios que se ajuste a la regla de caché de extracción, Amazon ECR utiliza la configuración predeterminada para el nuevo repositorio. Estas configuraciones predeterminadas incluyen desactivar la inmutabilidad de las etiquetas, utilizar el cifrado AES-256 y no aplicar ninguna política de repositorio o ciclo de vida.

El uso de una plantilla de creación de repositorios con un prefijo que coincida con una regla de caché de extracción le permite definir los ajustes que Amazon ECR aplica a los nuevos repositorios creados mediante la acción de caché de extracción. Puede definir la inmutabilidad de las etiquetas, la configuración del cifrado, los permisos de los repositorios, la política de ciclo de vida y las etiquetas de recursos para los nuevos repositorios.

En el siguiente diagrama, se muestra el flujo de trabajo que Amazon ECR usa cuando se usa una plantilla de creación de repositorio.



A continuación se describe en detalle cada parámetro de una plantilla de creación de repositorios.

Prefix

El prefijo es el prefijo del espacio de nombres del repositorio que se va a asociar a la plantilla. A todos los repositorios creados con este prefijo se les aplicará la configuración definida en esta plantilla. Por ejemplo, el prefijo de `prod` se aplicaría a todos los repositorios que comiencen por `prod/`. De forma similar, el prefijo de `prod/team` se aplicaría a todos los repositorios que comiencen por `prod/team/`.

Para aplicar una plantilla a todos los repositorios de su registro que no tengan una plantilla de creación asociada, puede utilizar `ROOT` como prefijo.

Important

Siempre se aplica una suposición `/` al final del prefijo. Si especifica `ecr-public` como prefijo, Amazon ECR lo tratará como `ecr-public/`. Cuando utilice una regla de caché de extracción, el prefijo de repositorio que especifique durante la creación de la regla es el que debe especificar también como prefijo de la plantilla de creación de repositorios.

Descripción

Esta descripción de la plantilla es opcional y se utiliza para describir el propósito de la plantilla de creación de repositorios.

Versión de plantilla

La versión de la plantilla de creación de repositorios que se va a utilizar. Actualmente, solo se admite la versión de plantilla `TV1`.

Versión de configuración

La versión de configuración del repositorio es la plantilla que se va a utilizar. Cada plantilla debe incluir una configuración de repositorio. La versión de configuración predeterminada es `CV1` y consiste en los ajustes de mutabilidad de las etiquetas de imagen, política de repositorio y política de ciclo de vida.

Mutabilidad de etiquetas de imágenes

La configuración de mutabilidad de etiquetas que se utilizará en los repositorios creados con la plantilla. Si se omite este parámetro, se utilizará la configuración predeterminada de `MUTABLE`, lo que permitirá sobrescribir las etiquetas de imágenes. Esta es la configuración recomendada para

las plantillas utilizadas en los repositorios creados mediante acciones de caché de extracción. Esto garantiza que Amazon ECR pueda actualizar las imágenes almacenadas en caché cuando las etiquetas sean las mismas.

Si se especifica INMUTABLE, todas las etiquetas de imagen dentro del repositorio serán inmutables, lo que evitará que se sobrescriban.

La configuración de cifrado

La configuración de cifrado que se utilizará en los repositorios creados con la plantilla.

Si utiliza el tipo de cifrado de KMS, el contenido del repositorio se cifrará mediante el cifrado de lado del servidor con la clave de AWS Key Management Service almacenada en AWS KMS. Cuando utiliza AWS KMS para cifrar sus datos, puede utilizar la AWS KMS clave AWS gestionada predeterminada para Amazon ECR o especificar su propia AWS KMS clave, que ya ha creado. Para obtener más información, consulte [Protección de datos mediante el cifrado del lado del servidor con una AWS Key Management Service clave almacenada en AWS Key Management Service \(SSE-KMS\) en la Guía del usuario](#) de Amazon Simple Storage Service.

Si utiliza el tipo de cifrado AES256, Amazon ECR utiliza el cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 que cifran las imágenes del repositorio mediante un algoritmo de cifrado AES-256. Para obtener más información, consulte [Protección de datos mediante el cifrado del lado del servidor con las claves de cifrado administradas por Amazon S3 \(SSE-S3\)](#) en la Guía del usuario de Amazon Simple Storage Service.

Permisos de repositorio

La política de repositorios que se aplicará a los repositorios creados con la plantilla. Una política de repositorio utiliza permisos basados en recursos para controlar el acceso a un repositorio. Los permisos basados en recursos permiten especificar qué usuarios o roles de IAM tienen acceso a un repositorio y qué acciones pueden realizar en él. De forma predeterminada, solo la AWS cuenta que creó el repositorio tiene acceso a un repositorio. Puede aplicar un documento de política que otorgue o deniegue permisos adicionales a su repositorio. Para obtener más información, consulte [Políticas de repositorios privados en Amazon ECR](#).

Política del ciclo de vida de repositorio

La política de ciclo de vida que se utilizará para los repositorios creados con la plantilla. Una política de ciclo de vida proporciona más control sobre la administración del ciclo de vida de las imágenes en un repositorio privado. Una política de ciclo de vida incluye una o varias reglas, en la que cada regla define una acción de Amazon ECR. Esto proporciona una forma de automatizar

la limpieza de sus imágenes de contenedor, cuyo vencimiento se produce en función de su antigüedad o recuento. Para obtener más información, consulte [Automatice la limpieza de imágenes mediante políticas de ciclo de vida en Amazon ECR](#).

Etiquetas de recursos

Las etiquetas de recursos son metadatos que se aplican a los repositorios para ayudarlo a categorizarlos y organizarlos. Cada etiqueta está formada por una clave y un valor opcional, ambos definidos por el usuario.

Permisos de IAM para crear plantillas de creación de repositorios

Los siguientes permisos son necesarios para que una entidad principal de IAM administre las plantillas de creación de repositorios. Este permiso debe otorgarse a través de una política de IAM basada en identidad.

- `ecr:CreateRepositoryCreationTemplate`: otorga permiso para crear una plantilla de creación de repositorio.
- `ecr>DeleteRepositoryCreationTemplate`: otorga permiso para eliminar una plantilla de creación de repositorio.
- `ecr:PutLifecyclePolicy`: otorga permiso para crear una política de ciclo de vida y aplicarla a un repositorio. Este permiso solo es necesario si la plantilla de creación del repositorio incluye una política de ciclo de vida.
- `ecr:SetRepositoryPolicy`: otorga permiso para crear una política de permisos para un repositorio. Este permiso solo es necesario si la plantilla de creación del repositorio incluye una política de repositorio.
- `ecr:TagResource`: concede permiso para agregar etiquetas de metadatos a un recurso. Este permiso solo es necesario si la plantilla de creación del repositorio incluye etiquetas de recursos.

Creación de una plantilla de creación de repositorios en Amazon ECR

Puede crear una plantilla de creación de repositorio para definir la configuración que se utilizará en los repositorios creados por Amazon ECR en su nombre durante las acciones de caché de extracción. Una vez creada la plantilla de creación de repositorios, se aplicará la configuración a todos los repositorios nuevos que se creen durante las acciones de extracción de la memoria caché. Esto no tiene ningún efecto en ningún repositorio creado anteriormente.

Crear una plantilla de creación de repositorios (AWS Management Console)

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/>.
2. En la barra de navegación, elija la región en la que crear la plantilla de creación del repositorio.
3. En el panel de navegación, elija Registro privado, Plantillas de creación de repositorios.
4. En la página de plantillas de creación de repositorios, seleccione Crear plantilla.
5. En la página del Paso 1: Definir una plantilla, en Detalles de la plantilla, elija Un prefijo específico para aplicar la plantilla a un prefijo de espacio de nombres de repositorio específico o elija Cualquier prefijo de su registro de ECR para aplicar la plantilla a todos los repositorios que no coincidan con ninguna otra plantilla de la región.
 - a. Si elige Un prefijo específico, especifique el prefijo del espacio de nombres del repositorio al que se va a aplicar la plantilla en Prefijo. Siempre se aplica una suposición / al final del prefijo. Por ejemplo, el prefijo de `prod` se aplicaría a todos los repositorios que comiencen por `prod/`. De forma similar, el prefijo de `prod/team` se aplicaría a todos los repositorios que comiencen por `prod/team/`.
 - b. Si selecciona Cualquier prefijo en su registro ECR, el Prefijo se establecerá en `ROOT`.
6. En Descripción de la plantilla, especifique una descripción opcional para la plantilla y, a continuación, seleccione Siguiente.
7. En la página del Paso 2: Agregar la configuración de creación de repositorios, especifique la configuración del repositorio que se aplicará a los repositorios creados con la plantilla.
 - a. Para Mutabilidad de la etiqueta de imagen, elija la configuración de mutabilidad de la etiqueta que desea utilizar. Para obtener más información, consulte [Evitar que las etiquetas de imagen se sobrescriban en Amazon ECR](#).


Cuando se selecciona Mutable, las etiquetas de imagen se pueden sobrescribir. Esta es la configuración recomendada para las plantillas utilizadas en los repositorios creados mediante acciones de caché de extracción. Esto garantiza que Amazon ECR pueda actualizar las imágenes almacenadas en caché cuando las etiquetas sean las mismas.

Cuando se selecciona Inmutable, se evita que las etiquetas de imagen se sobrescriban. Una vez que el repositorio está configurado con etiquetas inmutables, se devuelve un error `ImageTagAlreadyExistsException` si se intenta insertar una imagen con una etiqueta que ya existe en el repositorio. Cuando la inmutabilidad de etiquetas está encendida para un repositorio, esto afecta a todas las etiquetas y no puede hacer que algunas etiquetas sean inmutables mientras que otras no lo son.

- b. Para Configuración del cifrado, elija el ajuste de cifrado que desee utilizar. Para obtener más información, consulte [Cifrado en reposo](#).

Cuando se selecciona AES-256, Amazon ECR utiliza cifrado del lado del servidor con claves de cifrado administradas por Amazon Simple Storage Service que cifra sus datos en reposo mediante un algoritmo de cifrado AES-256 estándar de la industria. Esto se ofrece sin costo adicional.

Cuando se selecciona AWS KMS, Amazon ECR utiliza el cifrado del lado del servidor con las claves almacenadas en AWS Key Management Service ().AWS KMS Cuando utiliza AWS KMS para cifrar sus datos, puede utilizar la clave AWS gestionada predeterminada, que gestiona Amazon ECR, o especificar su propia AWS KMS clave, que se denomina clave gestionada por el cliente.

 Note

La configuración de cifrado de un repositorio no se puede cambiar una vez creado el repositorio.

- c. En Permisos del repositorio, especifique la política de permisos del repositorio que se aplicará a los repositorios creados con esta plantilla. Si lo desea, puede utilizar el menú desplegable para seleccionar uno de los ejemplos de JSON para los casos de uso más comunes. Para obtener más información, consulte [Políticas de repositorios privados en Amazon ECR](#).
 - d. En Política de ciclo de vida del repositorio, especifique la política de ciclo de vida del repositorio que se aplicará a los repositorios creados con esta plantilla. Si lo desea, puede utilizar el menú desplegable para seleccionar uno de los ejemplos de JSON para los casos de uso más comunes. Para obtener más información, consulte [Automatice la limpieza de imágenes mediante políticas de ciclo de vida en Amazon ECR](#).
 - e. En el caso de las AWS etiquetas de repositorio, especifique los metadatos, en forma de pares clave-valor, que desee asociar a los repositorios creados con esta plantilla y, a continuación, seleccione Siguiente. Para obtener más información, consulte [Etiquetado de un repositorio privado en Amazon ECR](#).
8. En la página del Paso 3: Revisar y crear, revise la configuración que especificó para la plantilla de creación del repositorio. Seleccione la opción Editar para realizar cambios. Cuando haya terminado, elija Crear.

Eliminar una plantilla de creación de repositorios en Amazon ECR

Puede eliminar una plantilla de creación de repositorios si ha terminado de utilizarla. Una vez eliminada la plantilla de creación de repositorios, se aplicará la configuración predeterminada a todos los repositorios que se creen durante una acción de extracción de la memoria caché.

Eliminar una plantilla de creación de repositorios (AWS Management Console)

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/>.
2. En la barra de navegación, elija la región en la que se encuentra la plantilla de creación del repositorio que desea eliminar.
3. En el panel de navegación, elija Registro privado, Plantillas de creación de repositorios.
4. En la página de plantillas de creación de repositorios, seleccione la plantilla de creación de repositorios que desee eliminar.
5. En el menú desplegable Acciones, elija Eliminar.

Validación de las reglas de extracción de caché en Amazon ECR

Después de crear una regla de extracción de memoria caché, en el caso de los registros ascendentes que requieren autenticación, puede validar que la regla funcione correctamente. Al validar una regla de extracción de caché, Amazon ECR establece una conexión de red con el registro principal, comprueba que puede acceder al secreto de Secrets Manager que contiene las credenciales del registro ascendente y verifica que la autenticación se haya realizado correctamente.

Antes de empezar a trabajar con las reglas de caché extraíble, compruebe que dispone de los permisos de IAM adecuados. Para obtener más información, consulte [Se requieren permisos de IAM para sincronizar un registro ascendente con un registro privado de Amazon ECR](#).

Para validar una regla de caché de extracción (AWS Management Console)

Los siguientes pasos muestran cómo crear una regla de caché de extracción mediante la consola de Amazon ECR.

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/>.
2. En la barra de navegación, elija la región que contiene la regla de caché de extracción que desea validar.

3. En el panel de navegación, elija Private registry (Registro privado), Pull through cache (Caché de extracción).
4. En la página de Configuración de caché de extracción, seleccione la regla de caché de extracción que desee validar. A continuación, usa el menú desplegable Acciones y selecciona Ver detalles.
5. En la página de detalles de la regla de caché de extracción, use el menú desplegable Acciones y seleccione Verificar la autenticación. Amazon ECR mostrará un banner con el resultado.
6. Repita estos pasos para cada regla de caché de extracción que desee validar.

Para validar una regla de caché de extracción (AWS CLI)

El AWS CLI comando [validate-pull-through-cache-rule se utiliza para validar una regla](#) de extracción de caché para un registro privado de Amazon ECR. En el siguiente ejemplo, se utiliza `ecr-public` el prefijo del espacio de nombres. Sustituya ese valor por el valor de prefijo de la regla de caché de extracción que desee validar.

```
aws ecr validate-pull-through-cache-rule \  
  --ecr-repository-prefix ecr-public \  
  --region us-east-2
```

En la respuesta, el `isValid` parámetro indica si la validación se ha realizado correctamente o no. Si es `true`, Amazon ECR pudo acceder al registro principal y la autenticación se realizó correctamente. Si `false`, se ha producido un problema y la validación ha fallado. El `failure` parámetro indica la causa.

Extracción de una imagen con una regla de extracción de caché en Amazon ECR

En los ejemplos siguientes se muestra la sintaxis del comando que se debe utilizar al extraer una imagen mediante una regla de caché de extracción. Si aparece un error al extraer una imagen ascendente mediante una regla de caché de extracción, consulte [Solución de problemas de extracción de memoria caché en Amazon ECR](#) para ver los errores más habituales y cómo resolverlos.

Antes de empezar a trabajar con las reglas de extracción de caché, compruebe que dispone de los permisos de IAM adecuados. Para obtener más información, consulte [Se requieren permisos de IAM para sincronizar un registro ascendente con un registro privado de Amazon ECR](#).

Note

En los ejemplos siguientes se utilizan los valores de espacio de nombres del repositorio de Amazon ECR predeterminados que utilizan. AWS Management Console Asegúrese de utilizar el URI del repositorio privado de Amazon ECR que ha configurado.

Para Amazon ECR Public

```
docker pull aws_account_id.dkr.ecr.region.amazonaws.com/ecr-public/repository_name/  
image_name:tag
```

Kubernetes Container Registry

```
docker pull aws_account_id.dkr.ecr.region.amazonaws.com/kubernetes/repository_name/  
image_name:tag
```

Quay

```
docker pull aws_account_id.dkr.ecr.region.amazonaws.com/quay/repository_name/  
image_name:tag
```

Docker Hub

Para ver las imágenes oficiales de Docker Hub:

```
docker pull aws_account_id.dkr.ecr.region.amazonaws.com/docker-hub/  
library/image_name:tag
```

Note

En el caso de las imágenes oficiales de Docker Hub, se debe `/library` incluir el prefijo. Para todos los demás repositorios de Docker Hub, debes omitir el prefijo. `/library`

Para el resto de imágenes de Docker Hub:

```
docker pull aws_account_id.dkr.ecr.region.amazonaws.com/docker-hub/repository_name/  
image_name:tag
```

GitHub Registro de contenedores

```
docker pull aws_account_id.dkr.ecr.region.amazonaws.com/github/repository_name/  
image_name:tag
```

Para Microsoft Azure Container Registry

```
docker pull aws_account_id.dkr.ecr.region.amazonaws.com/azure/repository_name/  
image_name:tag
```

GitLab Registro de contenedores

```
docker pull aws_account_id.dkr.ecr.region.amazonaws.com/gitlab/repository_name/  
image_name:tag
```

Almacenar en secreto las credenciales del repositorio principal AWS Secrets Manager

Al crear una regla de caché de extracción para un repositorio ascendente que requiera autenticación, debe almacenar las credenciales en un secreto de Secrets Manager. El uso de un secreto de Secrets Manager puede tener un coste. Para más información, consulte [Precios de AWS Secrets Manager](#).


Los siguientes procedimientos explican cómo crear un secreto de Secrets Manager para cada repositorio upstream compatible. Si lo desea, puede utilizar el flujo de trabajo de creación de reglas de caché de extracción en la consola de Amazon ECR para crear el secreto en lugar de crearlo mediante la consola Secrets Manager. Para obtener más información, consulte [Creación de una regla de extracción de caché en Amazon ECR](#).

Docker Hub


Para crear un secreto de Secrets Manager para tus credenciales de Docker Hub (AWS Management Console)

1. Abra la consola de Secrets Manager en <https://console.aws.amazon.com/secretsmanager/>.
2. Elija Almacenar un secreto nuevo.

3. En la página Elegir tipo de secreto, haga lo siguiente:
 - a. En Secret type (Tipo de secreto), elija Other type of secret (Otro tipo de secreto).
 - b. En pares clave/valor, cree dos filas para sus credenciales de Docker Hub. Puede almacenar hasta 65536 bytes en el secreto.
 - i. Para el primer par clave/valor, especifíquelo `username` como clave y su nombre de usuario de Docker Hub como valor.
 - ii. Para el primer par clave/valor, especifíquelo `accessToken` como clave y su nombre de usuario de Docker Hub como valor. Para obtener más información sobre cómo crear un token de acceso de Docker Hub, consulta [Crear y administrar los tokens de acceso](#) en la documentación de Docker.
 - c. En el caso de la clave de cifrado, mantenga el valor predeterminado de `aws/secretsmanager` AWS KMS key y, a continuación, seleccione Siguiente. No se aplica ningún cargo por el uso de esta clave. Para obtener más información, consulte [Cifrado y descifrado secretos en Secrets Manager](#) en la Guía del AWS Secrets Manager usuario.

 Important

Debe utilizar la clave de `aws/secretsmanager` cifrado predeterminada para cifrar su secreto. Amazon ECR no permite usar una clave administrada por el cliente (CMK) para esto.

4. En la página Configurar el secreto, haga lo siguiente:
 - a. Ingrese un Nombre de secreto descriptivo y una Descripción. Los nombres de los secretos deben contener de 1 a 512 caracteres Unicode con el prefijo `ecr-pullthroughcache/`.
-  Important
- El Amazon ECR AWS Management Console solo muestra los secretos de Secrets Manager cuyos nombres utilizan el `ecr-pullthroughcache/` prefijo.
- b. (Opcional) En la sección Tags (Etiquetas), agregue etiquetas a su secreto. Para conocer las estrategias de etiquetado, consulte [los secretos de Tag Secrets Manager](#) en la Guía del AWS Secrets Manager usuario. No almacene información confidencial en etiquetas porque no están cifradas.

- c. (Opcional) En Resource permissions (Permisos de recursos), para agregar una política de recursos a su secreto, elija Edit permissions (Editar permisos). Para obtener más información, consulte [Adición de una política de permisos a un secreto](#) en la Guía del usuario de AWS Secrets Manager .
 - d. (Opcional) En Replicar secreto, para replicar su secreto en otra persona Región de AWS, elija Replicar secreto. Puede replicar el secreto ahora o volver y replicarlo más tarde. Para obtener más información, consulte [Replicar un secreto a otras regiones](#) en la Guía del usuario de AWS Secrets Manager .
 - e. Elija Siguiente.
5. (Opcional) En la página Configure rotation (Configurar rotación), puede activar la rotación automática. También puede mantener la rotación desactivada por ahora y activarla más tarde. Para obtener más información, consulte [Rotar secretos de Secrets Manager](#) en la Guía del usuario de AWS Secrets Manager . Elija Siguiente.
 6. En la página Review (Revisar), revise los detalles del secreto y, a continuación, elija Store (Almacenar).


Secrets Manager vuelve a la lista de secretos. Si el nuevo secreto no aparece, elija el botón Refresh (Actualizar).

GitHub Container Registry

Para crear un secreto de Secrets Manager para tus credenciales de GitHub Container Registry (AWS Management Console)

1. Abra la consola de Secrets Manager en <https://console.aws.amazon.com/secretsmanager/>.
2. Elija Almacenar un secreto nuevo.
3. En la página Elegir tipo de secreto, haga lo siguiente:
 - a. En Secret type (Tipo de secreto), elija Other type of secret (Otro tipo de secreto).
 - b. En pares clave/valor, cree dos filas para sus GitHub credenciales. Puede almacenar hasta 65536 bytes en el secreto.
 - i. Para el primer par clave/valor, especifique username como clave y su GitHub nombre de usuario como valor.
 - ii. Para el segundo par clave/valor, especifique accessToken como clave y su token de GitHub acceso como valor. Para obtener más información sobre cómo crear un

- token de GitHub acceso, consulte [Administrar sus tokens de acceso personales](#) en la GitHub documentación.
- c. En el caso de la clave de cifrado, mantenga el valor predeterminado de `aws/secretsmanager` AWS KMS key y, a continuación, seleccione Siguiente. No se aplica ningún cargo por el uso de esta clave. Para obtener más información, consulte [Cifrado y descifrado secretos en Secrets Manager](#) en la Guía del AWS Secrets Manager usuario.

 Important

Debe utilizar la clave de `aws/secretsmanager` cifrado predeterminada para cifrar su secreto. Amazon ECR no permite usar una clave administrada por el cliente (CMK) para esto.

4. En la página Configure secret (Configurar el secreto), haga lo siguiente:
 - a. Ingrese un Nombre de secreto descriptivo y una Descripción. Los nombres de los secretos deben contener de 1 a 512 caracteres Unicode con el prefijo `ecr-pullthroughcache/`.

 Important

El Amazon ECR AWS Management Console solo muestra los secretos de Secrets Manager cuyos nombres utilizan el `ecr-pullthroughcache/` prefijo.

- b. (Opcional) En la sección Tags (Etiquetas), agregue etiquetas a su secreto. Para conocer las estrategias de etiquetado, consulte [los secretos de Tag Secrets Manager](#) en la Guía del AWS Secrets Manager usuario. No almacene información confidencial en etiquetas porque no están cifradas.
- c. (Opcional) En Resource permissions (Permisos de recursos), para agregar una política de recursos a su secreto, elija Edit permissions (Editar permisos). Para obtener más información, consulte [Adición de una política de permisos a un secreto](#) en la Guía del usuario de AWS Secrets Manager .
- d. (Opcional) En Replicar secreto, para replicar su secreto en otra persona Región de AWS, elija Replicar secreto. Puede replicar el secreto ahora o volver y replicarlo más tarde. Para obtener más información, consulte [Replicar un secreto a otras regiones](#) en la Guía del usuario de AWS Secrets Manager .
- e. Elija Siguiente.

5. (Opcional) En la página Configure rotation (Configurar rotación), puede activar la rotación automática. También puede mantener la rotación desactivada por ahora y activarla más tarde. Para obtener más información, consulte [Rotar secretos de Secrets Manager](#) en la Guía del usuario de AWS Secrets Manager . Elija Siguiente.
6. En la página Review (Revisar), revise los detalles del secreto y, a continuación, elija Store (Almacenar).

Secrets Manager vuelve a la lista de secretos. Si el nuevo secreto no aparece, elija el botón Refresh (Actualizar).

Microsoft Azure Container Registry

Para crear un secreto de Secrets Manager para sus credenciales de Microsoft Azure Container Registry (AWS Management Console)

1. Abra la consola de Secrets Manager en <https://console.aws.amazon.com/secretsmanager/>.
2. Elija Almacenar un secreto nuevo.
3. En la página Elegir tipo de secreto, haga lo siguiente:
 - a. En Secret type (Tipo de secreto), elija Other type of secret (Otro tipo de secreto).
 - b. En pares clave/valor, cree dos filas para sus credenciales de GitHub. Puede almacenar hasta 65536 bytes en el secreto.
 - i. Para el primer par clave/valor, especifíquelo `username` como clave y su nombre de usuario de Microsoft Azure Container Registry como valor.
 - ii. Para el primer par clave/valor, especifíquelo `accessToken` como clave y su nombre de usuario de Microsoft Azure Container Registry como valor. Para obtener más información sobre la creación de un token de acceso a Microsoft Azure Container Registry, consulte [Crear token: portal](#) en la documentación de Microsoft Azure.
 - c. En el caso de la clave de cifrado, mantenga el valor predeterminado de `aws/secretsmanager` AWS KMS key y, a continuación, seleccione Siguiente. No se aplica ningún cargo por el uso de esta clave. Para obtener más información, consulte [Cifrado y descifrado secretos en Secrets Manager](#) en la Guía del AWS Secrets Manager usuario.

⚠ Important

Debe utilizar la clave de `aws/secretsmanager` cifrado predeterminada para cifrar su secreto. Amazon ECR no permite usar una clave administrada por el cliente (CMK) para esto.

4. En la página Configure secret (Configurar el secreto), haga lo siguiente:
 - a. Ingrese un Nombre de secreto descriptivo y una Descripción. Los nombres de los secretos deben contener de 1 a 512 caracteres Unicode con el prefijo `ecr-pullthroughcache/`.

⚠ Important

El Amazon ECR AWS Management Console solo muestra los secretos de Secrets Manager cuyos nombres utilizan el `ecr-pullthroughcache/` prefijo.

- b. (Opcional) En la sección Tags (Etiquetas), agregue etiquetas a su secreto. Para conocer las estrategias de etiquetado, consulte [los secretos de Tag Secrets Manager](#) en la Guía del AWS Secrets Manager usuario. No almacene información confidencial en etiquetas porque no están cifradas.
 - c. (Opcional) En Resource permissions (Permisos de recursos), para agregar una política de recursos a su secreto, elija Edit permissions (Editar permisos). Para obtener más información, consulte [Adición de una política de permisos a un secreto](#) en la Guía del usuario de AWS Secrets Manager .
 - d. (Opcional) En Replicar secreto, para replicar su secreto en otra persona Región de AWS, elija Replicar secreto. Puede replicar el secreto ahora o volver y replicarlo más tarde. Para obtener más información, consulte [Replicar un secreto a otras regiones](#) en la Guía del usuario de AWS Secrets Manager .
 - e. Elija Siguiente.
 5. (Opcional) En la página Configure rotation (Configurar rotación), puede activar la rotación automática. También puede mantener la rotación desactivada por ahora y activarla más tarde. Para obtener más información, consulte [Rotar secretos de Secrets Manager](#) en la Guía del usuario de AWS Secrets Manager . Elija Siguiente.
 6. En la página Review (Revisar), revise los detalles del secreto y, a continuación, elija Store (Almacenar).

Secrets Manager vuelve a la lista de secretos. Si el nuevo secreto no aparece, elija el botón Refresh (Actualizar).

GitLab Container Registry

Para crear un secreto de Secrets Manager para tus credenciales de GitLab Container Registry (AWS Management Console)

1. Abra la consola de Secrets Manager en <https://console.aws.amazon.com/secretsmanager/>.
2. Elija Almacenar un secreto nuevo.
3. En la página Elegir tipo de secreto, haga lo siguiente:
 - a. En Secret type (Tipo de secreto), elija Other type of secret (Otro tipo de secreto).
 - b. En pares clave/valor, cree dos filas para sus GitLab credenciales. Puede almacenar hasta 65536 bytes en el secreto.
 - i. Para el primer par clave/valor, especifíquelo `username` como clave y su nombre de usuario de GitLab Container Registry como valor.
 - ii. Para el segundo par clave/valor, especifíquelo `accessToken` como clave y su token de acceso a GitLab Container Registry como valor. Para obtener más información sobre la creación de un token de acceso a GitLab Container Registry, consulta los [identificadores de acceso personal](#), los [identificadores de acceso grupal](#) o los [identificadores de acceso a proyectos](#) en la GitLab documentación.
 - c. En el caso de la clave de cifrado, mantenga el valor predeterminado de `aws/secretsmanager` AWS KMS key y, a continuación, seleccione Siguiente. No se aplica ningún cargo por el uso de esta clave. Para obtener más información, consulte [Cifrado y descifrado secretos en Secrets Manager](#) en la Guía del AWS Secrets Manager usuario.

Important

Debe utilizar la clave de `aws/secretsmanager` cifrado predeterminada para cifrar su secreto. Amazon ECR no permite usar una clave administrada por el cliente (CMK) para esto.

4. En la página Configure secret (Configurar el secreto), haga lo siguiente:

- a. Ingrese un Nombre de secreto descriptivo y una Descripción. Los nombres de los secretos deben contener de 1 a 512 caracteres Unicode con el prefijo `ecr-pullthroughcache/`.

 Important

El Amazon ECR AWS Management Console solo muestra los secretos de Secrets Manager cuyos nombres utilizan el `ecr-pullthroughcache/` prefijo.

- b. (Opcional) En la sección Tags (Etiquetas), agregue etiquetas a su secreto. Para conocer las estrategias de etiquetado, consulte [los secretos de Tag Secrets Manager](#) en la Guía del AWS Secrets Manager usuario. No almacene información confidencial en etiquetas porque no están cifradas.
 - c. (Opcional) En Resource permissions (Permisos de recursos), para agregar una política de recursos a su secreto, elija Edit permissions (Editar permisos). Para obtener más información, consulte [Adición de una política de permisos a un secreto](#) en la Guía del usuario de AWS Secrets Manager .
 - d. (Opcional) En Replicar secreto, para replicar su secreto en otra persona Región de AWS, elija Replicar secreto. Puede replicar el secreto ahora o volver y replicarlo más tarde. Para obtener más información, consulte [Replicar un secreto a otras regiones](#) en la Guía del usuario de AWS Secrets Manager .
 - e. Elija Siguiente.
5. (Opcional) En la página Configure rotation (Configurar rotación), puede activar la rotación automática. También puede mantener la rotación desactivada por ahora y activarla más tarde. Para obtener más información, consulte [Rotar secretos de Secrets Manager](#) en la Guía del usuario de AWS Secrets Manager . Elija Siguiente.
 6. En la página Review (Revisar), revise los detalles del secreto y, a continuación, elija Store (Almacenar).

Secrets Manager vuelve a la lista de secretos. Si el nuevo secreto no aparece, elija el botón Refresh (Actualizar).

Solución de problemas de extracción de memoria caché en Amazon ECR

Cuando se extrae una imagen ascendente mediante una regla de caché de extracción, los errores que aparecen con más frecuencia son los siguientes.

El repositorio no existe

Un error que indica que el repositorio no existe suele deberse bien a que el repositorio no existe en el registro privado de Amazon ECR o bien a que no se ha otorgado el permiso `ecr:CreateRepository` a la entidad principal de IAM que realiza la extracción de la imagen ascendente. Para resolver este error, se debe verificar que el URI del repositorio del comando de extracción es correcto, que se han otorgado los permisos de IAM necesarios a la entidad principal que realiza la extracción de la imagen ascendente o que el repositorio donde se va a insertar la imagen ascendente se ha creado en el registro privado de Amazon ECR antes de realizar el extracción de la imagen ascendente. Para obtener más información sobre los permisos de IAM necesarios, consulte [Se requieren permisos de IAM para sincronizar un registro ascendente con un registro privado de Amazon ECR](#).

A continuación se muestra un ejemplo de este error.

```
Error response from daemon: repository 111122223333.dkr.ecr.us-east-1.amazonaws.com/
ecr-public/amazonlinux/amazonlinux not found: name unknown: The repository with
name 'ecr-public/amazonlinux/amazonlinux' does not exist in the registry with id
'111122223333'
```

No se encontró la imagen solicitada

Un error que indica que no se puede encontrar la imagen suele deberse bien a que la imagen no existe en el registro ascendente o bien a que no se ha otorgado el permiso `ecr:BatchImportUpstreamImage` a la entidad principal de IAM que realiza la extracción de la imagen ascendente, aunque el repositorio ya se va a crear en el registro privado de Amazon ECR. Para resolver este error, se debe verificar que la imagen ascendente y el nombre de la etiqueta de la imagen son correctos y existen, así como que se han otorgado los permisos de IAM necesarios a la entidad principal de IAM que realiza la extracción de la imagen ascendente. Para obtener más información sobre los permisos de IAM necesarios, consulte [Se requieren permisos de IAM para sincronizar un registro ascendente con un registro privado de Amazon ECR](#).

A continuación se muestra un ejemplo de este error.

```
Error response from daemon: manifest for 111122223333.dkr.ecr.us-east-1.amazonaws.com/ecr-public/amazonlinux/amazonlinux:latest not found: manifest unknown: Requested image not found
```

403 Prohibido cuando se extrae de un repositorio de Docker Hub

Cuando extraiga datos de un repositorio de Docker Hub que esté etiquetado como imagen oficial de Docker, debe incluir `/library/` en la URI que utilices. Por ejemplo, `aws_account_id.dkr.ecr.region.amazonaws.com/docker-hub/library/image_name:tag`. Si omite `/library/` para las imágenes oficiales de Docker Hub, aparecerá un error 403 Forbidden cuando intente extraer una imagen mediante una regla de caché de extracción. Para obtener más información, consulte [Extracción de una imagen con una regla de extracción de caché en Amazon ECR](#).

A continuación se muestra un ejemplo de este error.

```
Error response from daemon: failed to resolve reference "111122223333.dkr.ecr.us-west-2.amazonaws.com/docker-hub/amazonlinux:2023": pulling from host 111122223333.dkr.ecr.us-west-2.amazonaws.com failed with status code [manifests 2023]: 403 Forbidden
```

Replicación de imágenes privadas en Amazon ECR

Puede configurar el registro privado de Amazon ECR para que admita la replicación de los repositorios. Amazon ECR admite la replicación entre regiones y entre cuentas. Para que se produzca la replicación entre cuentas, la cuenta de destino debe configurar una política de permisos de registro con objeto de permitir que se produzca la replicación desde el registro de origen. Para obtener más información, consulte [Permisos de registro privado en Amazon ECR](#).

Temas

- [Consideraciones sobre la replicación de imágenes privadas](#)
- [Ejemplos de replicación de imágenes privadas para Amazon ECR](#)
- [Configuración de la replicación privada de imágenes en Amazon ECR](#)

Consideraciones sobre la replicación de imágenes privadas

Al utilizar la replicación de imágenes privadas, se debe tener en cuenta lo siguiente.

- Solo se replica el contenido del repositorio insertado en un repositorio una vez configurada la replicación. El contenido preexistente en un repositorio no se replica. Una vez configurada la replicación para un repositorio, Amazon ECR mantiene sincronizados el destino y el origen.
- El nombre del repositorio seguirá siendo el mismo en todas las regiones y cuentas cuando se produzca la replicación. Amazon ECR no admite el cambio del nombre del repositorio durante la replicación.
- La primera vez que se configura el registro privado para la replicación, Amazon ECR crea un rol de IAM vinculado a servicios en su nombre. El rol de IAM vinculado a servicios otorga al servicio de replicación de Amazon ECR el permiso necesario para crear repositorios y replicar imágenes en el registro. Para obtener más información, consulte [Uso de roles vinculados a servicios para Amazon ECR](#).
- Para que se produzca la replicación entre cuentas, el destino del registro privado debe conceder permiso con objeto de permitir que el registro de origen replique sus imágenes. Para ello, se establece una política de permisos de registro privado. Para obtener más información, consulte [Permisos de registro privado en Amazon ECR](#).
- Si se cambia la política de permisos de un registro privado para quitar un permiso, se pueden completar las replications en curso concedidas anteriormente.

- Para que se produzca la replicación entre regiones, tanto la cuenta de origen como la de destino deben estar habilitadas en la región antes de que se lleve a cabo cualquier acción de replicación dentro o hacia esa región. Para obtener más información, consulte [Administración de las regiones de AWS](#) en la Referencia general de Amazon Web Services.
- No se admite la replicación entre regiones entre particiones. AWS Por ejemplo, no se puede replicar un repositorio us-west-2 en cn-north-1. Para obtener más información sobre AWS las particiones, consulte el [formato ARN](#) en la Referencia AWS general.
- La configuración de replicación de un registro privado puede contener hasta 25 destinos únicos en todas las reglas, con un máximo de 10 reglas. Cada regla puede contener hasta 100 filtros. Esto permite especificar reglas independientes para repositorios que contienen imágenes utilizadas para la producción y las pruebas, por ejemplo.
- La configuración de replicación admite el filtrado de los repositorios de un registro privado que se replican especificando un prefijo de repositorio. Para ver un ejemplo, consulte [Ejemplo: Configurar la replicación entre regiones mediante un filtro de repositorio](#).
- Una acción de replicación solo se produce una vez por cada inserción de imagen. Por ejemplo, si ha configurado la replicación entre regiones desde us-west-2 hasta us-east-1 y de us-east-1 hasta us-east-2, una imagen insertada en us-west-2 se replicará solo en us-east-1, y no se replicará de nuevo en us-east-2. Este comportamiento se aplica a la replicación entre regiones y entre cuentas.
- La mayoría de las imágenes se replican en menos de 30 minutos, pero en casos excepcionales la replicación puede tardar más.
- La replicación del registro no realiza ninguna acción de eliminación. Las imágenes y repositorios replicados se pueden eliminar manualmente cuando ya no los utilice.
- Las políticas de repositorio, incluidas las políticas de IAM, así como las políticas de ciclo de vida, no se replican ni tienen ningún efecto en otro repositorio que no sea para el que están definidas.
- La configuración del repositorio no se replica. La inmutabilidad de etiquetas, el escaneo de imágenes y la configuración de cifrado KMS están deshabilitados de forma predeterminada en todos los repositorios creados debido a una acción de replicación. La configuración de inmutabilidad de etiquetas y de escaneo de imágenes se puede cambiar una vez creado el repositorio. No obstante, la configuración solo se aplica a las imágenes insertadas después de que la configuración haya cambiado.
- Si la inmutabilidad de etiquetas está habilitada en un repositorio y se replica una imagen que utiliza la misma etiqueta que una existente, la imagen se replica pero no incluirá la etiqueta duplicada. Esto podría provocar que la imagen se quedara sin etiquetar.

Ejemplos de replicación de imágenes privadas para Amazon ECR

Los siguientes ejemplos muestran casos de uso comunes para la replicación de imágenes privadas. Si configura la replicación mediante el AWS CLI, puede utilizar los ejemplos de JSON como punto de partida al crear el archivo JSON. Si configuras la replicación mediante el AWS Management Console, verás un JSON similar cuando revises la regla de replicación en la página Revisar y enviar.

Ejemplo: Configurar la replicación entre regiones en una única región de destino

A continuación se muestra un ejemplo para configurar la replicación entre regiones en un único registro. En este ejemplo, se presupone que el ID de cuenta es 111122223333 y que está especificando esta configuración de replicación en una región distinta de `us-west-2`.

```
{
  "rules": [
    {
      "destinations": [
        {
          "region": "us-west-2",
          "registryId": "111122223333"
        }
      ]
    }
  ]
}
```

Ejemplo: Configurar la replicación entre regiones mediante un filtro de repositorio

A continuación se muestra un ejemplo con objeto de configurar la replicación entre regiones para repositorios que coincidan con un valor de nombre de prefijo. En este ejemplo, se presupone que el ID de cuenta es 111122223333 y que está especificando esta configuración de replicación en una región distinta de `us-west-1` y que tiene repositorios con un prefijo `prod`.

```
{
  "rules": [{
    "destinations": [{
```



```
"region": "us-west-1",
"registryId": "111122223333"
}],
"repositoryFilters": [{
  "filter": "prod",
  "filterType": "PREFIX_MATCH"
}]
}]
}
```

Ejemplo: Configurar la replicación entre regiones en varias regiones de destino

A continuación se muestra un ejemplo para configurar la replicación entre regiones en un único registro. En este ejemplo se presupone que el ID de cuenta es 111122223333 y que está especificando esta configuración de replicación en una región distinta de us-west-1 o us-west-2.

```
{
  "rules": [
    {
      "destinations": [
        {
          "region": "us-west-1",
          "registryId": "111122223333"
        },
        {
          "region": "us-west-2",
          "registryId": "111122223333"
        }
      ]
    }
  ]
}
```

Ejemplo: Configurar la replicación entre cuentas

A continuación se muestra un ejemplo de configuración de la replicación entre cuentas para el registro. En este ejemplo se configura la replicación en la cuenta 444455556666 y en la región us-west-2.

⚠ Important

Para que se produzca la replicación entre cuentas, la cuenta de destino debe configurar una política de permisos de registro con objeto de permitir que se produzca la replicación. Para obtener más información, consulte [Permisos de registro privado en Amazon ECR](#).

```
{
  "rules": [
    {
      "destinations": [
        {
          "region": "us-west-2",
          "registryId": "444455556666"
        }
      ]
    }
  ]
}
```

Ejemplo: Especificar varias reglas en una configuración

A continuación se muestra un ejemplo de configuración de varias reglas de replicación para el registro. En este ejemplo se configura la replicación para la cuenta **111122223333**, con una regla que replica repositorios con un prefijo `prod` en la región `us-west-2` y repositorios con un prefijo `test` en la región `us-east-2`. Una configuración de replicación puede incluir hasta 10 reglas, y cada regla puede especificar hasta 25 destinos.

```
{
  "rules": [{
    "destinations": [{
      "region": "us-west-2",
      "registryId": "111122223333"
    }],
    "repositoryFilters": [{
      "filter": "prod",
      "filterType": "PREFIX_MATCH"
    }]
  },
  {
    "destinations": [{
```

```
"region": "us-east-2",
"registryId": "111122223333"
}],
"repositoryFilters": [{
  "filter": "test",
  "filterType": "PREFIX_MATCH"
}]
}
]
}
```

Configuración de la replicación privada de imágenes en Amazon ECR

Configure la replicación por región para su registro privado. Puede configurar la replicación entre regiones o entre cuentas.

Para ver ejemplos de cómo se usa habitualmente la replicación, consulte [Ejemplos de replicación de imágenes privadas para Amazon ECR](#).

Configuración de las opciones de replicación del registro (AWS Management Console)

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/repositories>.
2. En la barra de navegación, elija la región en la que se va a configurar la política de replicación del registro.
3. En el panel de navegación, elija Private registry (Registro privado).
4. En la página Private registry (Registro privado), en la sección Replication (Replicación), elija Edit (Editar).
5. En la página Replication (Replicación), elija Add replication rule (Agregar regla de replicación).
6. En la página Destination types (Tipos de destino), elija si desea habilitar la replicación entre regiones, entre cuentas o ambas y, a continuación, elija Next (Siguiente).
7. Si está habilitada la replicación entre regiones, en Configure destination regions (Configurar regiones de destino) elija una o varias Destination regions (Regiones de destino) y luego Next (Siguiente).
8. Si está habilitada la replicación entre cuentas, en Cross-account replication (Replicación entre cuentas) elija la configuración de replicación entre cuentas del registro. En Destination account (Cuenta de destino), ingrese el ID de cuenta de la cuenta de destino y una o varias Destination

regions (Regiones de destino) en las que se vaya a replicar. Elija Destination account + (Cuenta de destino +) para configurar cuentas adicionales como destinos de replicación.

⚠ Important

Para que se produzca la replicación entre cuentas, la cuenta de destino debe configurar una política de permisos de registro con objeto de permitir que se produzca la replicación. Para obtener más información, consulte [Permisos de registro privado en Amazon ECR](#).

9. (Opcional) En la página Add filters (Agregar filtros), especifique uno o más filtros para la regla de replicación y, a continuación, elija Add (Agregar). Repita este paso para cada filtro que desee asociar a la acción de replicación. Se debe especificar un filtro como prefijo del nombre del repositorio. Si no se agrega ningún filtro, se replicará el contenido de todos los repositorios. Elija Next (Siguiente) una vez que se hayan agregado todos los filtros.
10. En la página Review and submit (Revisar y enviar), revise la configuración de regla de replicación y luego elija Submit rule (Enviar regla).

Configuración de las opciones de replicación del registro (AWS CLI)

1. Cree un archivo JSON que incluya las reglas de replicación que se definirán para el registro. Una configuración de replicación puede contener hasta 10 reglas, con hasta 25 destinos exclusivos para todas las reglas y 100 filtros por cada regla. Para configurar la replicación entre regiones en de su propia cuenta, especifique su propio ID de cuenta. Para obtener más ejemplos, consulte [Ejemplos de replicación de imágenes privadas para Amazon ECR](#).

```
{
  "rules": [{
    "destinations": [{
      "region": "destination_region",
      "registryId": "destination_accountId"
    }],
    "repositoryFilters": [{
      "filter": "repository_prefix_name",
      "filterType": "PREFIX_MATCH"
    }]
  }]
}
```

2. Cree una configuración de replicación para el registro.

```
aws ecr put-replication-configuration \  
  --replication-configuration file://replication-settings.json \  
  --region us-west-2
```

3. Confirme la configuración del registro.

```
aws ecr describe-registry \  
  --region us-west-2
```

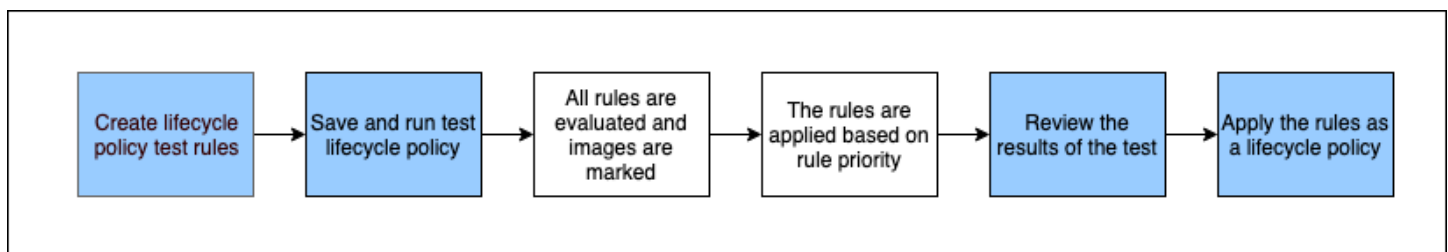
Automatice la limpieza de imágenes mediante políticas de ciclo de vida en Amazon ECR

Las políticas de ciclo de vida de Amazon ECR proporcionan un mayor control sobre la administración del ciclo de vida de las imágenes en un repositorio privado. Una política de ciclo de vida contiene una o más reglas y cada regla define una acción para Amazon ECR. Según los criterios de caducidad de la política de ciclo de vida, las imágenes caducan en función de su antigüedad o recuento en un plazo de 24 horas. Cuando Amazon ECR realiza una acción basada en una política de ciclo de vida, esta acción se captura como un evento en AWS CloudTrail. Para obtener más información, consulte [Registrar las acciones de Amazon ECR con AWS CloudTrail](#).

Funcionamiento de las políticas de ciclo de vida

Una política de ciclo de vida se compone de una o varias reglas que determinan las imágenes de un repositorio que se deben marcar para vencimiento. Al plantearse el uso de políticas de ciclo de vida, es importante utilizar la vista previa de las políticas de ciclo de vida para confirmar qué imágenes marcará la política de ciclo de vida para vencimiento antes de aplicarla a un repositorio. Una vez que se aplica una política de ciclo de vida a un repositorio, lo normal es que las imágenes caduquen en un plazo de 24 horas tras haber cumplido con los criterios de caducidad. Cuando Amazon ECR realiza una acción basada en una política de ciclo de vida, se captura como un evento en AWS CloudTrail. Para obtener más información, consulte [Registrar las acciones de Amazon ECR con AWS CloudTrail](#).

En el siguiente diagrama se muestra el flujo de trabajo de una política de ciclo de vida.



1. Cree una o varias reglas de prueba.
2. Guarde las reglas de prueba y ejecute la vista previa.
3. El evaluador de políticas de ciclo de vida revisa todas las reglas y marca las imágenes a las que afecta cada regla.

4. A continuación, el evaluador de políticas de ciclo de vida aplica las reglas, en función de la prioridad de la regla, y muestra qué imágenes del repositorio están configuradas para que se marquen para vencimiento.
5. Revise los resultados de la prueba, asegurándose de que las imágenes marcadas para vencimiento sean las previstas.
6. Aplique las reglas de prueba como la política de ciclo de vida del repositorio.
7. Una vez creada una política de ciclo de vida, lo normal es que las imágenes caduquen en un plazo de 24 horas tras haber cumplido con los criterios de caducidad.

Reglas de evaluación de políticas de ciclo de vida

El evaluador de políticas de ciclo de vida se encarga de analizar el código JSON en texto sin formato de la política de ciclo de vida, de evaluar todas las reglas y de aplicarlas en función de la prioridad de regla a las imágenes en el repositorio. A continuación se explica la lógica del evaluador de políticas de ciclo de vida con más detalle. Para ver ejemplos, consulte [Ejemplos de políticas de ciclo de vida en Amazon ECR](#).

- Todas las reglas se evalúan al mismo tiempo, independientemente de la prioridad. Después de evaluar todas las reglas, se aplican en función de la prioridad.
- Una imagen puede ser marcada para vencimiento exactamente por una o ninguna regla.
- Una imagen que cumpla los requisitos de etiquetado de una regla no puede ser marcada para vencimiento por una regla con una prioridad menor.
- Las reglas no pueden marcar nunca imágenes que están marcadas con reglas de mayor prioridad, pero puede seguir identificándolas si no han caducado.
- El conjunto de reglas debe contener un conjunto único de prefijos de etiqueta.
- Solo una regla puede seleccionar imágenes sin etiquetar.
- Si una lista de manifiestos hace referencia a una imagen, no puede caducar sin que se elimine primero la lista de manifiestos.
- El vencimiento se ordena siempre por `pushed_at_time` y las imágenes más antiguas caducan siempre antes que las más nuevas.
- Una regla de política de ciclo de vida puede especificar `tagPatternList` o `tagPrefixList`, pero no ambas. Sin embargo, una política de ciclo de vida puede contener varias reglas, y las diferentes reglas utilizan listas de patrones y prefijos.

- Los parámetros `tagPatternList` o `tagPrefixList` solo se pueden usar si `tagStatus` es `tagged`.
- Cuando se utiliza `tagPatternList`, una imagen se considera que coincide correctamente si coincide con el filtro comodín. Por ejemplo, si se aplica un filtro de `prod*`, coincidirá con los repositorios cuyo nombre comience con `prod`, como `prod`, `prod1` o `production-team1`. Del mismo modo, si se aplica un filtro de `*prod*`, coincidirá con los repositorios cuyo nombre contenga `prod`, por ejemplo `repo-production` o `prod-team`.

Important

Hay un límite máximo de cuatro caracteres comodines (*) por cadena. Por ejemplo, `["*test*1*2*3", "test*1*2*3*"]` es válido pero `["test*1*2*3*4*5*6"]` no es válido.

- Cuando se utiliza `tagPrefixList`, se encuentra una coincidencia de una imagen si todas las etiquetas del valor de `tagPrefixList` coinciden con todas las etiquetas de la imagen.
- El parámetro `countUnit` solo se utiliza si `countType` es `sinceImagePushed`.
- Con `countType = imageCountMoreThan`, las imágenes se ordenan de las más nuevas a las más antiguas en función de `pushed_at_time` y se marcan para vencimiento todas las imágenes mayores que el recuento especificado.
- Con `countType = sinceImagePushed`, todas las imágenes cuyo `pushed_at_time` sea anterior al número de días especificado basado en `countNumber` se marcan para vencimiento.

Creación de una vista previa de la política de ciclo de vida en Amazon ECR

Puede utilizar una vista previa de la política de ciclo de vida para ver el impacto de una política de ciclo de vida en un repositorio de imágenes antes de aplicarla. Se considera una práctica recomendada realizar una vista previa antes de aplicar una política de ciclo de vida a un repositorio.

Note

Si utiliza la replicación de Amazon ECR para realizar copias de un repositorio en distintas regiones o cuentas, tenga en cuenta que una política de ciclo de vida solo puede tomar medidas en los repositorios de la región en la que se creó. Por lo tanto, si tiene activada la

replicación, puede considerar la posibilidad de crear una política de ciclo de vida en cada región y cuenta en la que vaya a replicar sus repositorios.

Creación de una vista previa de política de ciclo de vida (AWS Management Console)

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/repositories>.
2. En la barra de navegación, seleccione la región que contiene el repositorio en el que desea obtener la vista previa de una política de ciclo de vida.
3. En el panel de navegación, en Registro privado, elija Repositorios.
4. En la página Repositorios privados, seleccione un repositorio y luego utilice el menú desplegable Acciones para elegir las políticas del ciclo de vida.
5. En la página de las reglas de la política de ciclo de vida del repositorio, elija Editar reglas de prueba, Crear regla.
6. Especifique los siguientes detalles para cada regla de la política de ciclo de vida.
 - a. En Rule priority (Prioridad de la regla), escriba un número para la prioridad de la regla. La prioridad de la regla determina el orden en el que se aplican las reglas de la política del ciclo de vida.
 - b. En Rule description (Descripción de la regla), escriba una descripción para la regla de política de ciclo de vida.
 - c. En el estado de la imagen, elija Etiquetada (coincidencia de comodines), Etiquetada (coincidencia de prefijos), Sin etiquetar o Cualquiera.
 - d. Si selecciona Etiquetado (coincidencia de comodines) para el estado de la imagen y, a continuación, en Especificar etiquetas para la coincidencia de comodines, puede especificar una lista de etiquetas de imagen con un comodín (*) sobre las que ejecutar una acción según su política de ciclo de vida. Por ejemplo, si las imágenes están etiquetadas como prod, prod1, prod2, etc., debería especificar prod* para ejecutar una acción en todas ellas. Si especifica varias etiquetas, solo se seleccionan las imágenes con todas las etiquetas especificadas.

⚠ Important

Hay un límite máximo de cuatro caracteres comodines (*) por cadena. Por ejemplo, ["*test*1*2*3", "test*1*2*3*"] es válido pero ["test*1*2*3*4*5*6"] no es válido.

- e. Si selecciona Etiquetado (coincidencia de prefijos) para el estado de la imagen y, a continuación, en Especificar etiquetas para la coincidencia de prefijos, puede especificar una lista de etiquetas de imagen para ejecutar una acción según su política de ciclo de vida.
 - f. En los criterios de coincidencia, seleccione Desde que se envió la imagen o Número de imágenes superior a, a continuación, especifique un valor.
 - g. Seleccione Guardar.
7. Cree reglas de política de ciclo de vida de prueba adicionales repitiendo los pasos 5–7.
 8. Para ejecutar la vista previa de la política de ciclo de vida, elija Save and run test (Guardar y ejecutar prueba).
 9. En Image matches for test lifecycle rules (Coincidencias de imagen para reglas de ciclo de vida de prueba), revise el impacto de la vista previa de la política de ciclo de vida.
 10. Si está conforme con los resultados de la vista preliminar, elija Apply as lifecycle policy para crear una política de ciclo de vida con las reglas especificadas. Una vez aplicada una política de ciclo de vida, las imágenes a las que afecta esta política vencen en un plazo de 24 horas.
 11. Si no le convencen los resultados de la vista previa, puede eliminar una o más reglas del ciclo de vida de las pruebas y crear una o más reglas para reemplazarlas y, a continuación, repetir la prueba.

Creación de una política de ciclo de vida para un repositorio en Amazon ECR

Usa una política de ciclo de vida para crear un conjunto de reglas que hagan caducar las imágenes del repositorio no utilizadas. Tras crear una política de ciclo de vida, las imágenes afectadas caducan en 24 horas.

Note

Si utiliza la replicación de Amazon ECR para realizar copias de un repositorio en distintas regiones o cuentas, tenga en cuenta que una política de ciclo de vida solo puede tomar medidas en los repositorios de la región en la que se creó. Por lo tanto, si tiene activada la replicación, puede considerar la posibilidad de crear una política de ciclo de vida en cada región y cuenta en la que vaya a replicar sus repositorios.

Requisito previo

Práctica recomendada: cree una vista previa de la política de ciclo de vida para comprobar que las imágenes que han caducado según las normas de su política de ciclo de vida cumplen sus expectativas. Para ver instrucciones, consulte [Creación de una vista previa de la política de ciclo de vida en Amazon ECR](#).

Creación de una política de ciclo de vida (AWS Management Console)

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/repositories>.
2. En la barra de navegación, seleccione la región que contiene el repositorio para el que desea crear una política de ciclo de vida.
3. En el panel de navegación, en Registro privado, elija Repositorios.
4. En la página Repositorios privados, seleccione un repositorio y luego utilice el menú desplegable Acciones para elegir las políticas del ciclo de vida.
5. En la página de política de ciclo de vida del repositorio, elija Crear regla.
6. Especifique los siguientes detalles para la regla de la política de ciclo de vida.
 - a. En Rule priority (Prioridad de la regla), escriba un número para la prioridad de la regla. La prioridad de la regla determina el orden en el que se aplican las reglas de la política del ciclo de vida.
 - b. En Rule description (Descripción de la regla), escriba una descripción para la regla de política de ciclo de vida.
 - c. En el estado de la imagen, elija Etiquetada (coincidencia de comodines), Etiquetada (coincidencia de prefijos), Sin etiquetar o Cualquiera.
 - d. Si selecciona Etiquetado (coincidencia de comodines) para el estado de la imagen y, a continuación, en Especificar etiquetas para la coincidencia de comodines, puede especificar

una lista de etiquetas de imagen con un comodín (*) sobre las que ejecutar una acción según su política de ciclo de vida. Por ejemplo, si las imágenes están etiquetadas como prod, prod1, prod2, etc., debería especificar prod* para ejecutar una acción en todas ellas. Si especifica varias etiquetas, solo se seleccionan las imágenes con todas las etiquetas especificadas.

⚠ Important

Hay un límite máximo de cuatro caracteres comodines (*) por cadena. Por ejemplo, ["*test*1*2*3", "test*1*2*3*"] es válido pero ["test*1*2*3*4*5*6"] no es válido.

- e. Si selecciona Etiquetado (coincidencia de prefijos) para el estado de la imagen y, a continuación, en Especificar etiquetas para la coincidencia de prefijos, puede especificar una lista de etiquetas de imagen sobre las que actuar según su política de ciclo de vida.
 - f. En los criterios de coincidencia, seleccione Desde que se envió la imagen o Número de imágenes superior a, a continuación, especifique un valor.
 - g. Elija Save (Guardar).
7. Cree reglas de política de ciclo de vida adicionales repitiendo los pasos 5–7.

Creación de una política de ciclo de vida (AWS CLI)

1. Obtenga el nombre del repositorio para el que va a crear la política de ciclo de vida.

```
aws ecr describe-repositories
```

2. Cree un archivo local denominado policy.json con el contenido de la política de ciclo de vida. Para ver ejemplos de política de ciclo de vida, consulte [Ejemplos de políticas de ciclo de vida en Amazon ECR](#).
3. Cree una política de ciclo de vida especificando el nombre del repositorio y haga referencia al archivo JSON de la política de ciclo de vida que ha creado.

```
aws ecr put-lifecycle-policy \  
  --repository-name repository-name \  
  --lifecycle-policy-text file://policy.json
```

Ejemplos de políticas de ciclo de vida en Amazon ECR

A continuación se muestran ejemplos de políticas de ciclo de vida que muestran la sintaxis.

Para obtener más información sobre las propiedades de las políticas, consulte [Propiedades de la política de ciclo de vida en Amazon ECR](#). Para obtener instrucciones sobre cómo crear una política de ciclo de vida mediante el AWS CLI, consulte [Creación de una política de ciclo de vida \(AWS CLI\)](#).

Plantilla de política de ciclo de vida

El contenido de su política de ciclo de vida se evalúa antes de asociarlo a un repositorio. A continuación, se muestra la plantilla de sintaxis JSON de la política de ciclo de vida.

```
{
  "rules": [
    {
      "rulePriority": integer,
      "description": "string",
      "selection": {
        "tagStatus": "tagged"|"untagged"|"any",
        "tagPatternList": list<string>,
        "tagPrefixList": list<string>,
        "countType": "imageCountMoreThan"|"sinceImagePushed",
        "countUnit": "string",
        "countNumber": integer
      },
      "action": {
        "type": "expire"
      }
    }
  ]
}
```

Filtrar por antigüedad de las imágenes

En el siguiente ejemplo, se muestra la sintaxis de la política de ciclo de vida de una política que crea el vencimiento de las imágenes con una etiqueta que comienza con prod al usar una tagPatternList de prod* que también tienen más de 14 días.

```
{
```

```
"rules": [  
  {  
    "rulePriority": 1,  
    "description": "Expire images older than 14 days",  
    "selection": {  
      "tagStatus": "tagged",  
      "tagPatternList": ["prod*"],  
      "countType": "sinceImagePushed",  
      "countUnit": "days",  
      "countNumber": 14  
    },  
    "action": {  
      "type": "expire"  
    }  
  }  
]  
}
```

Filtrar por el número de imágenes

En el siguiente ejemplo se muestra la sintaxis de una política de ciclo de vida que conserva solo una imagen sin etiquetar y marca para vencimiento todas las demás:

```
{  
  "rules": [  
    {  
      "rulePriority": 1,  
      "description": "Keep only one untagged image, expire all others",  
      "selection": {  
        "tagStatus": "untagged",  
        "countType": "imageCountMoreThan",  
        "countNumber": 1  
      },  
      "action": {  
        "type": "expire"  
      }  
    }  
  ]  
}
```

Filtrar por varias reglas

El siguiente ejemplo usa varias reglas en una política de ciclo de vida. Se ofrece un repositorio de ejemplo y una política de ciclo de vida con una explicación del resultado.

Ejemplo A

Contenido del repositorio:

- Imagen A, lista de etiquetas: ["beta-1", "prod-1"], insertada: hace 10 días
- Imagen B, lista de etiquetas: ["beta-2", "prod-2"], insertada: hace 9 días
- Imagen C, lista de etiquetas: ["beta-3"], insertada: hace 8 días

Texto de la política de ciclo de vida:

```
{
  "rules": [
    {
      "rulePriority": 1,
      "description": "Rule 1",
      "selection": {
        "tagStatus": "tagged",
        "tagPatternList": ["prod*"],
        "countType": "imageCountMoreThan",
        "countNumber": 1
      },
      "action": {
        "type": "expire"
      }
    },
    {
      "rulePriority": 2,
      "description": "Rule 2",
      "selection": {
        "tagStatus": "tagged",
        "tagPatternList": ["beta*"],
        "countType": "imageCountMoreThan",
        "countNumber": 1
      },
      "action": {
        "type": "expire"
      }
    }
  ]
}
```

```

    }
  }
]
}

```

La lógica de esta política de vida sería:

- La regla 1 identifica las imágenes etiquetadas con el prefijo prod. Debería marcar las imágenes, empezando por la más antigua, hasta que queden una o menos imágenes. Marca la imagen A para vencimiento.
- La regla 2 identifica las imágenes etiquetadas con el prefijo beta. Debería marcar las imágenes, empezando por la más antigua, hasta que queden una o menos imágenes. Marca la imagen A y la imagen B para vencimiento. Sin embargo, la imagen A ya ha sido identificada por la regla 1 y, si la imagen B se marcara para vencimiento, se infringiría la regla 1, por lo que se omite.
- Resultado: la imagen A se marca para vencimiento

Ejemplo B

Este es el mismo repositorio que el del ejemplo anterior, pero se ha cambiado el orden de prioridad de las reglas para ilustrar el resultado.

Contenido del repositorio:

- Imagen A, lista de etiquetas: ["beta-1", "prod-1"], insertada: hace 10 días
- Imagen B, lista de etiquetas: ["beta-2", "prod-2"], insertada: hace 9 días
- Imagen C, lista de etiquetas: ["beta-3"], insertada: hace 8 días

Texto de la política de ciclo de vida:

```

{
  "rules": [
    {
      "rulePriority": 1,
      "description": "Rule 1",
      "selection": {
        "tagStatus": "tagged",
        "tagPatternList": ["beta*"],
        "countType": "imageCountMoreThan",

```



```

        "countNumber": 1
    },
    "action": {
        "type": "expire"
    }
},
{
    "rulePriority": 2,
    "description": "Rule 2",
    "selection": {
        "tagStatus": "tagged",
        "tagPatternList": ["prod*"],
        "countType": "imageCountMoreThan",
        "countNumber": 1
    },
    "action": {
        "type": "expire"
    }
}
]
}

```

La lógica de esta política de vida sería:

- La regla 1 identifica las imágenes etiquetadas con el prefijo beta. Debería marcar las imágenes, empezando por la más antigua, hasta que queden una o menos imágenes. Se identifican las tres imágenes, y la imagen A y la imagen B se marcan para vencimiento.
- La regla 2 identifica las imágenes etiquetadas con el prefijo prod. Debería marcar las imágenes, empezando por la más antigua, hasta que queden una o menos imágenes. No se identifica ninguna imagen porque todas las imágenes disponibles ya han sido identificadas por la regla 1, por lo que no se marcan imágenes adicionales.
- Resultado: la imagen A y la imagen B se marcan para vencimiento.

Filtrar por varias etiquetas en una sola regla

Los siguientes ejemplos especifican la sintaxis de la política de ciclo de vida para varios patrones de etiqueta en una sola regla. Se ofrece un repositorio de ejemplo y una política de ciclo de vida con una explicación del resultado.

Ejemplo A

Cuando se especifican varios patrones de etiqueta en una sola regla, las imágenes deben coincidir con todos los patrones de etiqueta especificados.

Contenido del repositorio:

- Imagen A, lista de etiquetas: ["alpha-1"], insertada: hace 12 días
- Imagen B, lista de etiquetas: ["beta-1"], insertada: hace 11 días
- Imagen C, lista de etiquetas: ["alpha-2", "beta-2"], insertada: hace 10 días
- Imagen D, lista de etiquetas: ["alpha-3"], insertada: hace 4 días
- Imagen E, lista de etiquetas: ["beta-3"], insertada: hace 3 días
- Imagen F, lista de etiquetas: ["alpha-4", "beta-4"], insertada: hace 2 días

```
{
  "rules": [
    {
      "rulePriority": 1,
      "description": "Rule 1",
      "selection": {
        "tagStatus": "tagged",
        "tagPatternList": ["alpha*", "beta*"],
        "countType": "sinceImagePushed",
        "countNumber": 5,
        "countUnit": "days"
      },
      "action": {
        "type": "expire"
      }
    }
  ]
}
```

La lógica de esta política de vida sería:

- La regla 1 identifica las imágenes etiquetadas con el prefijo `alpha` y `beta`. Se identifican las imágenes C y F y se marcan las imágenes que tienen más de cinco días (la imagen C).
- Resultado: la imagen C se marca para vencimiento

Ejemplo B

El ejemplo siguiente ilustra que las etiquetas no son exclusivas.

Contenido del repositorio:

- Imagen A, lista de etiquetas: ["alpha-1", "beta-1", "gamma-1"], insertada: hace 10 días
- Imagen B, lista de etiquetas: ["alpha-2", "beta-2"], insertada: hace 9 días
- Imagen C, lista de etiquetas: ["alpha-3", "beta-3", "gamma-2"], insertada: hace 8 días

```
{
  "rules": [
    {
      "rulePriority": 1,
      "description": "Rule 1",
      "selection": {
        "tagStatus": "tagged",
        "tagPatternList": ["alpha*", "beta*"],
        "countType": "imageCountMoreThan",
        "countNumber": 1
      },
      "action": {
        "type": "expire"
      }
    }
  ]
}
```

La lógica de esta política de vida sería:

- La regla 1 identifica las imágenes etiquetadas con el prefijo `alpha` y `beta`. Se identifican todas las imágenes. Debería marcar las imágenes, empezando por la más antigua, hasta que queden una o menos imágenes. Se marcan la imagen A y la imagen B para vencimiento.
- Resultado: la imagen A y la imagen B se marcan para vencimiento.

Filtrar por todas las imágenes

Los siguientes ejemplos de políticas de ciclo de vida especifican todas las imágenes con filtros distintos. Se ofrece un repositorio de ejemplo y una política de ciclo de vida con una explicación del resultado.

Ejemplo A

A continuación, se muestra la sintaxis de una política de ciclo de vida que se aplica a todas las reglas propiedad conserva solo una imagen sin etiquetar y marca para vencimiento todas las demás.

Contenido del repositorio:

- Imagen A, lista de etiquetas: ["alpha-1"], insertada: hace 4 días
- Imagen B, lista de etiquetas: ["beta-1"], insertada: hace 3 días
- Imagen C, lista de etiquetas: [], insertada: hace 2 días
- Imagen D, lista de etiquetas: ["alpha-2"], insertada: hace 1 día

```
{
  "rules": [
    {
      "rulePriority": 1,
      "description": "Rule 1",
      "selection": {
        "tagStatus": "any",
        "countType": "imageCountMoreThan",
        "countNumber": 1
      },
      "action": {
        "type": "expire"
      }
    }
  ]
}
```

La lógica de esta política de vida sería:

- La regla 1 identifica todas las imágenes. Detecta las imágenes A, B, C y D. Debe marcar para vencimiento todas las imágenes excepto la más reciente. Marca las imágenes A, B y C para vencimiento.

- Resultado: las imágenes A, B y C están vencidas.

Ejemplo B

El siguiente ejemplo ilustra una política de ciclo de vida que combina todos los tipos de reglas en una sola política.

Contenido del repositorio:

- Imagen A, lista de etiquetas: ["alpha-1", "beta-1"], insertada: hace 4 días
- Imagen B, lista de etiquetas: [], insertada: hace 3 días
- Imagen C, lista de etiquetas: ["alpha-2"], insertada: hace 2 días
- Imagen D, lista de etiquetas: ["git hash"], insertada: hace 1 día
- Imagen E, lista de etiquetas: [], insertada: hace 1 día

```
{
  "rules": [
    {
      "rulePriority": 1,
      "description": "Rule 1",
      "selection": {
        "tagStatus": "tagged",
        "tagPatternList": ["alpha"],
        "countType": "imageCountMoreThan",
        "countNumber": 1
      },
      "action": {
        "type": "expire"
      }
    },
    {
      "rulePriority": 2,
      "description": "Rule 2",
      "selection": {
        "tagStatus": "untagged",
        "countType": "sinceImagePushed",
        "countUnit": "days",
        "countNumber": 1
      },
      "action": {
```

```
        "type": "expire"
    }
},
{
    "rulePriority": 3,
    "description": "Rule 3",
    "selection": {
        "tagStatus": "any",
        "countType": "imageCountMoreThan",
        "countNumber": 1
    },
    "action": {
        "type": "expire"
    }
}
]
```

La lógica de esta política de vida sería:

- La regla 1 identifica las imágenes etiquetadas con el prefijo `alpha`. Identifica las imágenes A y C. Debe mantener la imagen más reciente y marcar el resto para vencimiento. Marca la imagen A para vencimiento.
- La regla 2 identifica las imágenes sin etiquetar. Identifica las imágenes B y E. Debe marcar todas las imágenes anteriores a un día para vencimiento. Marca la imagen B para vencimiento.
- La regla 3 identifica todas las imágenes. Identifica las imágenes A, B, C, D y E. Debe mantener la imagen más reciente y marcar el resto para vencimiento. Sin embargo, no puede marcar las imágenes A, B, C o E porque se identificaron con reglas de mayor prioridad. Marca la imagen D para vencimiento.
- Resultado: las imágenes A, B y D están vencidas.

Propiedades de la política de ciclo de vida en Amazon ECR

Las políticas de ciclo de vida tienen las siguientes propiedades.

Para ver ejemplos de políticas de ciclo de vida, consulte [Ejemplos de políticas de ciclo de vida en Amazon ECR](#). Para obtener instrucciones sobre cómo crear una política de ciclo de vida mediante el AWS CLI, consulte [Creación de una política de ciclo de vida \(AWS CLI\)](#).

Prioridad de las reglas

`rulePriority`

Tipo: número entero

Obligatorio: sí

Establece el orden en el que se aplican las reglas, de menor a mayor. Una regla de política de ciclo de vida con una prioridad de 1 se aplica primero, una regla con una prioridad de 2 es la siguiente, y así sucesivamente. Cuando añada reglas a una política de ciclo de vida, debe asignar a cada una un valor único para `rulePriority`. Los valores no tienen que ser secuenciales en todas las reglas de una política. Una regla con un valor `tagStatus` de `any` debe tener el valor más alto para `rulePriority` y evaluarse en último lugar.

Descripción

`description`

Tipo: string

Obligatorio: no

(Opcional) Describe la finalidad de una regla de una política de ciclo de vida.

Estado de etiqueta

`tagStatus`

Tipo: cadena

Obligatorio: sí

Determina si la regla de la política de ciclo de vida que añade especifica una etiqueta para una imagen. Las opciones válidas son `tagged`, `untagged` o `any`. Si especifica `any`, se evalúa la regla en todas las imágenes. Si especifica `tagged`, también debe especificar valor de `tagPrefixList`. Si especifica `untagged`, también debe omitir `tagPrefixList`.

Lista de patrones de etiquetas

tagPatternList

Tipo: lista[cadena]

Obligatorio: sí, en caso de que `tagStatus` esté configurado como etiquetado y `tagPrefixList` no está especificado

Al crear una política de ciclo de vida para las imágenes etiquetadas, se recomienda utilizar una `tagPatternList` para especificar cuáles son las etiquetas que van a caducar. Debe especificar una lista separada por comas de patrones de etiquetas de imagen que pueden contener comodines (*) en los que se va a realizar una acción con la política de ciclo de vida. Por ejemplo, si las imágenes están etiquetadas como `prod`, `prod1`, `prod2`, etc., debería usar la lista del patrón de etiqueta `prod*` para especificarlas todas. Si especifica varias etiquetas, solo se seleccionan las imágenes con todas las etiquetas especificadas.

Important

Hay un límite máximo de cuatro caracteres comodines (*) por cadena. Por ejemplo, `["*test*1*2*3", "test*1*2*3*"]` es válido pero `["test*1*2*3*4*5*6"]` no es válido.

Lista de prefijos de etiqueta

tagPrefixList

Tipo: lista[cadena]

Obligatorio: sí, en caso de que `tagStatus` esté configurado como etiquetado y `tagPatternList` no está especificado

Solo se usa si especificó `"tagStatus": "tagged"` y no está especificando un `tagPatternList`. Debe especificar una lista separada por comas de prefijos de etiquetas de imagen en los que se va a realizar una acción con la política de ciclo de vida. Por ejemplo, si las imágenes están etiquetadas como `prod`, `prod1`, `prod2`, etc., debería usar el prefijo de etiqueta `prod` para especificarlas todas. Si especifica varias etiquetas, solo se seleccionan las imágenes con todas las etiquetas especificadas.

Tipo de recuento

countType

Tipo: cadena

Obligatorio: sí

Especifique un tipo de recuento que desea aplicar a las imágenes.

Si `countType` está establecido en `imageCountMoreThan`, también especifica `countNumber` para crear una regla que establezca el límite de imágenes que hay en el repositorio. Si `countType` está establecido en `sinceImagePushed`, también especifica `countUnit` y `countNumber` para definir un límite de tiempo de las imágenes que hay en el repositorio.

Unidad de recuento

countUnit

Tipo: cadena

Obligatorio: sí, solo si `countType` está establecido en `sinceImagePushed`

Especifique una unidad de recuento de `days` para indicar la unidad de tiempo, además de `countNumber`, que es el número de días.

Solo debe especificarse cuando `countType` sea `sinceImagePushed`; se producirá un error si especifica una unidad de recuento cuando `countType` es otro valor.

Cantidad

countNumber

Tipo: número entero

Obligatorio: sí

Especifique un número de recuento. Los valores aceptables son enteros positivos (el valor 0 no se acepta).

Si el `countType` usado es `imageCountMoreThan`, el valor es el número máximo de imágenes que puede conservar en el repositorio. Si el `countType` usado es `sinceImagePushed`, el valor es el límite de antigüedad máxima de las imágenes.

Acción

`type`

Tipo: `string`

Obligatorio: sí

Especifique un tipo de acción. El valor admitido es `expire`.

Seguridad en Amazon Elastic Container Registry

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El [modelo de responsabilidad compartida](#) la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores independientes prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los [programas de conformidad de AWS](#). Para obtener más información sobre los programas de conformidad que se aplican a Amazon ECR, consulte [Servicios de AWS en el ámbito del programa de conformidad](#).
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación lo ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Amazon ECR. En los siguientes temas, se mostrará cómo configurar Amazon ECR para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus recursos de Amazon ECR.

Temas

- [Identity and Access Management para Amazon Elastic Container Registry](#)
- [Protección de los datos en Amazon ECR](#)
- [Validación de conformidad para Amazon Elastic Container Registry](#)
- [Seguridad de la infraestructura en Amazon Elastic Container Registry](#)
- [Prevención de la sustitución confusa entre servicios](#)

Identity and Access Management para Amazon Elastic Container Registry

AWS Identity and Access Management (IAM) es un sistema Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Amazon ECR. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

- [Público](#)
- [Autenticación con identidades](#)
- [Administración de acceso mediante políticas](#)
- [Cómo funciona Amazon Elastic Container Registry con IAM](#)
- [Ejemplos de políticas basadas en identidad de Amazon Elastic Container Registry](#)
- [Uso del control de acceso basado en etiquetas](#)
- [AWS políticas gestionadas para Amazon Elastic Container Registry](#)
- [Uso de roles vinculados a servicios para Amazon ECR](#)
- [Solución de problemas de identidad y acceso para Amazon Elastic Container Registry](#)

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realice en Amazon ECR.

Usuario de servicio: si utiliza el servicio Amazon ECR para realizar su trabajo, su administrador proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Amazon ECR para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica de Amazon ECR, consulte [Solución de problemas de identidad y acceso para Amazon Elastic Container Registry](#).

Administrador de servicio: si está a cargo de los recursos de Amazon ECR de su empresa, probablemente disponga de acceso completo a Amazon ECR. Su trabajo consiste en determinar

a qué características y recursos de Amazon ECR deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo la empresa puede utilizar IAM con Amazon ECR, consulte [Cómo funciona Amazon Elastic Container Registry con IAM](#).

Administrador de IAM: si es un administrador de IAM, es posible que desee obtener detalles sobre cómo escribir políticas para administrar el acceso a Amazon ECR. Para consultar ejemplos de políticas de Amazon ECR basadas en identidades que puede utilizar en IAM, consulte [Ejemplos de políticas basadas en identidad de Amazon Elastic Container Registry](#).

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (IAM Identity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte [Cómo iniciar sesión Cuenta de AWS en su](#) Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte [Firmar las solicitudes de la AWS API](#) en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte [Autenticación multifactor](#) en la Guía del usuario de AWS IAM Identity Center y [Uso de la autenticación multifactor \(MFA\) en AWS](#) en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte [Tareas que requieren credenciales de usuario raíz](#) en la Guía del usuario de IAM.

Usuarios y grupos de IAM

Un [usuario de IAM](#) es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte [Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración](#) en la Guía del usuario de IAM.

Un [grupo de IAM](#) es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte [Cuándo crear un usuario de IAM \(en lugar de un rol\)](#) en la Guía del usuario de IAM.

Roles de IAM

Un [rol de IAM](#) es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console [cambiando](#) de función. Puede

asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte [Uso de roles de IAM](#) en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- **Acceso de usuario federado:** para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte [Creación de un rol para un proveedor de identidades de terceros](#) en la Guía del usuario de IAM. Si utiliza IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte [Conjuntos de permisos](#) en la Guía del usuario de AWS IAM Identity Center .
- **Permisos de usuario de IAM temporales:** un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- **Acceso entre cuentas:** puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte [Cómo los roles de IAM difieren de las políticas basadas en recursos](#) en la Guía del usuario de IAM.
- **Acceso entre servicios:** algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
- **Sesiones de acceso directo (FAS):** cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para

obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte

[Reenviar sesiones de acceso](#).

- Rol de servicio: un rol de servicio es un [rol de IAM](#) que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte [Creación de un rol para delegar permisos a un Servicio de AWS](#) en la Guía del usuario de IAM.
- Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.
- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar una AWS función a una instancia EC2 y ponerla a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para más información, consulte [Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2](#) en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte [Cuándo crear un rol de IAM \(en lugar de un usuario\)](#) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte [Información general de políticas JSON](#) en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte [Creación de políticas de IAM](#) en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte [Elegir entre políticas administradas y políticas insertadas](#) en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe [especificar una entidad principal](#) en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- **Límites de permisos:** un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte [Límites de permisos para las entidades de IAM](#) en la Guía del usuario de IAM.
- **Políticas de control de servicios (SCP):** las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una. Usuario raíz de la cuenta de AWS Para obtener más información acerca de Organizations y las SCP, consulte [Funcionamiento de las SCP](#) en la Guía del usuario de AWS Organizations .
- **Políticas de sesión:** las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte [Políticas de sesión](#) en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo AWS determinar si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la [lógica de evaluación de políticas](#) en la Guía del usuario de IAM.

Cómo funciona Amazon Elastic Container Registry con IAM

Antes de utilizar IAM para administrar el acceso a Amazon ECR, debe conocer qué características de IAM se encuentran disponibles con Amazon ECR. Para obtener una visión general de cómo Amazon ECR y otros AWS servicios funcionan con IAM, consulte [AWS Servicios que funcionan con IAM en la Guía del usuario de IAM](#).

Temas

- [Políticas de Amazon ECR basadas en identidades](#)
- [Políticas basadas en recursos de Amazon ECR](#)
- [Autorización basada en etiquetas de Amazon ECR](#)
- [Roles de IAM de Amazon ECR](#)

Políticas de Amazon ECR basadas en identidades

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. Amazon ECR admite acciones, claves de condiciones y recursos específicos. Para obtener información sobre todos los elementos que utiliza en una política JSON, consulte [Referencia de los elementos de las políticas JSON de IAM](#) en la Guía del usuario de IAM.

Acciones

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Las acciones de políticas de Amazon ECR utilizan el siguiente prefijo antes de la acción: `ecr:`. Por ejemplo, para conceder a alguien permiso para crear un repositorio de Amazon ECR con la operación `CreateRepository` de la API de Amazon ECR, incluya la acción `ecr:CreateRepository` en su política. Las instrucciones de la política deben incluir un elemento

Action o un elemento NotAction. Amazon ECR define su propio conjunto de acciones que describen las tareas que se pueden realizar con este servicio.

Para especificar varias acciones en una única instrucción, sepárelas con comas del siguiente modo:

```
"Action": [  
    "ecr:action1",  
    "ecr:action2"
```

Puede utilizar caracteres comodín para especificar varias acciones (*). Por ejemplo, para especificar todas las acciones que comiencen con la palabra Describe, incluya la siguiente acción:

```
"Action": "ecr:Describe*"
```

Para ver una lista de las acciones de Amazon ECR, consulte [Acciones, recursos y claves de condiciones de Amazon Elastic Container Registry](#) en la Guía del usuario de IAM.

Recursos

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento Resource de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento Resource o NotResource. Como práctica recomendada, especifique un recurso utilizando el [Nombre de recurso de Amazon \(ARN\)](#). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*" 
```

Un recurso de repositorio de Amazon ECR tiene el siguiente ARN:

```
arn:${Partition}:ecr:${Region}:${Account}:repository/${Repository-name}
```

Para obtener más información sobre el formato de los ARN, consulte Nombres de [recursos de Amazon \(ARN\) y espacios de nombres de AWS servicio](#).

Por ejemplo, para especificar el repositorio `my-repo` en la región `us-east-1` en la instrucción, utilice el siguiente ARN:

```
"Resource": "arn:aws:ecr:us-east-1:123456789012:repository/my-repo"
```

Para especificar todos los repositorios que pertenecen a una cuenta específica, utilice el carácter comodín (*):

```
"Resource": "arn:aws:ecr:us-east-1:123456789012:repository/*"
```

Para especificar varios recursos en una única instrucción, separe los ARN con comas.

```
"Resource": [  
  "resource1",  
  "resource2"
```

Para ver una lista de los tipos de recursos de Amazon ECR y los ARN, consulte [Recursos definidos por Amazon Elastic Container Registry](#) en la Guía del usuario de IAM. Para obtener información acerca de las acciones con las que puede especificar el ARN de cada recurso, consulte [Acciones definidas por Amazon Elastic Container Registry](#).

Claves de condición

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen [operadores de condición](#), tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación AND lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una OR operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte [Elementos de la política de IAM: variables y etiquetas](#) en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de [contexto de condición AWS globales en la Guía](#) del usuario de IAM.

Amazon ECR define su propio conjunto de claves de condición y también admite el uso de algunas claves de condición globales. Para ver todas las claves de condición AWS globales, consulte las claves de [contexto de condición AWS globales](#) en la Guía del usuario de IAM.

La mayoría de las acciones de Amazon ECR admiten las claves de condición `aws:ResourceTag` y `ecr:ResourceTag`. Para obtener más información, consulte [Uso del control de acceso basado en etiquetas](#).

Para ver una lista de las claves de condición de Amazon ECR, consulte [Claves de condición definidas por Amazon Elastic Container Registry](#) en la Guía del usuario de IAM. Para obtener más información acerca de las acciones y los recursos con los que puede utilizar una clave de condición, consulte [Acciones definidas por Amazon Elastic Container Registry](#).

Ejemplos

Para ver ejemplos de políticas basadas en identidad de Amazon ECR, consulte [Ejemplos de políticas basadas en identidad de Amazon Elastic Container Registry](#).

Políticas basadas en recursos de Amazon ECR

Las políticas basadas en recursos son documentos de políticas JSON que especifican qué acciones puede realizar una entidad de servicio especificada en un recurso de Amazon ECR y en qué condiciones. Amazon ECR admite políticas de permisos basadas en recursos para repositorios de Amazon ECR. Las políticas basadas en recursos le permiten conceder a otras cuentas de permisos de uso para cada recurso. También puede utilizar una política basada en recursos para permitir a un servicio de AWS acceder a los repositorios de Amazon ECR.

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la [entidad principal de una política basada en recursos](#). Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación

de confianza. Si el principal y el recurso están en AWS cuentas diferentes, también debe conceder permiso a la entidad principal para acceder al recurso. Conceda permiso asociando a la entidad una política basada en identidades. Sin embargo, si la política basada en recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte [Cómo los roles de IAM difieren de las políticas basadas en recursos](#) en la Guía del usuario de IAM.

El servicio de Amazon ECR solo admite un tipo de política basada en recursos denominada política de repositorios, que se adjunta a un repositorio. Esta política indica las entidades principales (cuentas, usuarios, roles y usuarios federados) que pueden realizar acciones en el repositorio. Para obtener información sobre cómo asociar una política basada en recursos a un repositorio, consulte [Políticas de repositorios privados en Amazon ECR](#).

Note

En una política de repositorio de Amazon ECR, el elemento de política `Sid` admite caracteres y espacios adicionales que no se admiten en las políticas de IAM.

Ejemplos

Para ver ejemplos de políticas basadas en recursos de Amazon ECR, consulte [Ejemplos de políticas de repositorios privados en Amazon ECR](#).

Autorización basada en etiquetas de Amazon ECR

Puede adjuntar etiquetas a los recursos de Amazon ECR o transferirlas en una solicitud a Amazon ECR. Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el [elemento de condición](#) de una política utilizando las claves de condición `ecr:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`. Para obtener más información sobre el etiquetado de recursos de Amazon ECR, consulte [Etiquetado de un repositorio privado en Amazon ECR](#).

Para consultar un ejemplo de política basada en la identidad para limitar el acceso a un recurso en función de las etiquetas de ese recurso, consulte [Uso del control de acceso basado en etiquetas](#).

Roles de IAM de Amazon ECR

Un [rol de IAM](#) es una entidad de tu AWS cuenta que tiene permisos específicos.

Uso de credenciales temporales con Amazon ECR

Puede utilizar credenciales temporales para iniciar sesión con federación, asumir un rol de IAM o asumir un rol de acceso entre cuentas. Las credenciales de seguridad temporales se obtienen llamando a operaciones de la AWS STS API, como [AssumeRole](#) o [GetFederationToken](#).

Amazon ECR admite el uso de credenciales temporales.

Roles vinculados al servicio

Los [roles vinculados a un servicio](#) permiten a AWS los servicios acceder a los recursos de otros servicios para completar una acción en tu nombre. Los roles vinculados a servicios aparecen en la cuenta de IAM y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Amazon ECR admite roles vinculados a servicios. Para obtener más información, consulte [Uso de roles vinculados a servicios para Amazon ECR](#).

Ejemplos de políticas basadas en identidad de Amazon Elastic Container Registry

De manera predeterminada, los usuarios y roles no tienen permiso para crear ni modificar recursos de Amazon ECR. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS la API. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte [Creación de políticas de IAM](#) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por Amazon ECR, incluido el formato de los ARN para cada uno de los tipos de recursos, consulte [Acciones, recursos y claves de condición de Amazon Elastic Container Registry](#) en la Referencia de autorizaciones de servicio.

Para obtener información acerca de cómo crear una política basada en identidad de IAM con estos documentos de políticas JSON de ejemplo, consulte [Creación de políticas en la pestaña JSON](#) en la Guía del usuario de IAM.

Temas

- [Prácticas recomendadas relativas a políticas](#)
- [Uso de la consola de Amazon ECR](#)
- [Permitir a los usuarios ver sus propios permisos](#)
- [Acceso a un repositorio de Amazon ECR](#)

Prácticas recomendadas relativas a políticas

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar los recursos de Amazon ECR de su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las [políticas administradas por AWS](#) o las [políticas administradas por AWS para funciones de trabajo](#) en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte [Políticas y permisos en IAM](#) en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte [Elementos de la política de JSON de IAM: Condición](#) en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas

recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte [Política de validación de Analizador de acceso de IAM](#) en la Guía de usuario de IAM.

- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte [Configuración del acceso a una API protegido por MFA](#) en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las [Prácticas recomendadas de seguridad en IAM](#) en la Guía del usuario de IAM.

Uso de la consola de Amazon ECR

Para acceder a la consola de Amazon Elastic Container Registry, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de Amazon ECR de su AWS cuenta. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

Para garantizar que esas entidades puedan seguir utilizando la consola de Amazon ECR, añada la política AmazonEC2ContainerRegistryReadOnly AWS gestionada a las entidades. Para obtener más información, consulte [Agregar de permisos a un usuario](#) en la Guía del usuario de IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
        "ecr:BatchGetImage",
        "ecr:GetLifecyclePolicy",
```

```

        "ecr:GetLifecyclePolicyPreview",
        "ecr:ListTagsForResource",
        "ecr:DescribeImageScanFindings"
    ],
    "Resource": "*"
}
]
}

```

No es necesario conceder permisos mínimos de consola a los usuarios que solo realizan llamadas a la API AWS CLI o a la AWS API. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intenta realizar.

Permitir a los usuarios ver sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o AWS .

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",

```

```

        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
}

```

Acceso a un repositorio de Amazon ECR

En este ejemplo, quiere conceder a un usuario de su AWS cuenta acceso a uno de sus repositorios de Amazon ECR, `my-repo`. También desea permitir que el usuario inserte, extraiga y enumere imágenes.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListImagesInRepository",
      "Effect": "Allow",
      "Action": [
        "ecr:ListImages"
      ],
      "Resource": "arn:aws:ecr:us-east-1:123456789012:repository/my-repo"
    },
    {
      "Sid": "GetAuthorizationToken",
      "Effect": "Allow",
      "Action": [
        "ecr:GetAuthorizationToken"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ManageRepositoryContents",
      "Effect": "Allow",
      "Action": [
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",

```

```

        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
        "ecr:BatchGetImage",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:PutImage"
    ],
    "Resource": "arn:aws:ecr:us-east-1:123456789012:repository/my-repo"
}
]
}

```

Uso del control de acceso basado en etiquetas

La acción de la `CreateRepository` API Amazon ECR le permite especificar etiquetas al crear el repositorio. Para obtener más información, consulte [Etiquetado de un repositorio privado en Amazon ECR](#).

Para que los usuarios puedan etiquetar repositorios durante la creación, es preciso que tengan permisos para utilizar la acción que crea el recurso (por ejemplo, `ecr:CreateRepository`). Si se especifican etiquetas en la acción de creación de recursos, Amazon realiza una autorización adicional en la acción `ecr:CreateRepository` para verificar que los usuarios tengan permisos para crear etiquetas.

Puede utilizar el control de acceso basado en etiquetas con las políticas de IAM. A continuación se muestran algunos ejemplos.

La siguiente política solo permitiría a un usuario crear o etiquetar un repositorio como `key=environment, value=dev`.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCreateTaggedRepository",
      "Effect": "Allow",
      "Action": [
        "ecr:CreateRepository"
      ],
      "Resource": "*"
    }
  ]
}

```

```

    "Condition": {
      "StringEquals": {
        "aws:RequestTag/environment": "dev"
      }
    },
    {
      "Sid": "AllowTagRepository",
      "Effect": "Allow",
      "Action": [
        "ecr:TagResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/environment": "dev"
        }
      }
    }
  ]
}

```

La siguiente política permitiría a un usuario acceder a todos los repositorios a menos que estuvieran etiquetados como `key=environment,value=prod`.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ecr:*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": "ecr:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ecr:ResourceTag/environment": "prod"
        }
      }
    }
  ]
}

```

```
]
}
```

AWS políticas gestionadas para Amazon Elastic Container Registry

Una política AWS gestionada es una política independiente creada y administrada por AWS. Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir [políticas administradas por el cliente](#) específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte [Políticas administradas de AWS](#) en la Guía del usuario de IAM.

Amazon ECR proporciona varias políticas gestionadas que puede adjuntar a las identidades de IAM o a las instancias de Amazon EC2. Estas políticas gestionadas permiten distintos niveles de control sobre el acceso a los recursos de Amazon ECR y las operaciones de las API. Para obtener más información acerca de cada una de las operaciones de API mencionadas en estas políticas, consulte [Acciones](#) en la Referencia de la API de Amazon Elastic Container Registry.

Temas

- [AmazonEC2ContainerRegistryFullAccess](#)
- [AmazonEC2ContainerRegistryPowerUser](#)
- [AmazonEC2ContainerRegistryReadOnly](#)
- [AWSECRPullThroughCache_ServiceRolePolicy](#)
- [ECRReplicationServiceRolePolicy](#)
- [Amazon ECR actualiza las políticas AWS gestionadas](#)

AmazonEC2ContainerRegistryFullAccess

Puede adjuntar la política AmazonEC2ContainerRegistryFullAccess a las identidades de IAM.

Puede usar esta política administrada como punto de partida para crear su propia política de IAM en función de sus requisitos específicos. Por ejemplo, puede crear una política específica para proporcionar a un usuario o rol acceso completo de administrador con objeto de administrar el uso de Amazon ECR. Con la característica [Políticas de ciclo de vida de Amazon ECR](#), puede especificar la administración del ciclo de vida de las imágenes en un repositorio. Los eventos relacionados con las políticas del ciclo de vida se notifican como CloudTrail eventos. Amazon ECR está integrado AWS CloudTrail para que pueda mostrar los eventos de su política de ciclo de vida directamente en la consola de Amazon ECR. La política de IAM administrada AmazonEC2ContainerRegistryFullAccess incluye el permiso `cloudtrail:LookupEvents` para facilitar este comportamiento.

Detalles de los permisos

Esta política incluye los siguientes permisos:

- `ecr`: permite a las entidades de seguridad acceso completo a todas las API de Amazon ECR.
- `cloudtrail`— Permite a los directores buscar los eventos de administración o los eventos de AWS CloudTrail Insights capturados por ellos. CloudTrail

La política AmazonEC2ContainerRegistryFullAccess es como sigue.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecr:*",
        "cloudtrail:LookupEvents"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ]
    }
  ]
}
```



```

    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "iam:AWSServiceName": [
          "replication.ecr.amazonaws.com"
        ]
      }
    }
  }
]
}

```

AmazonEC2ContainerRegistryPowerUser

Puede adjuntar la política AmazonEC2ContainerRegistryPowerUser a las identidades de IAM.

Esta política otorga permisos administrativos que permiten que los usuarios de IAM lean y escriban en los repositorios, pero no les permite eliminar los repositorios ni cambiar los documentos de la política aplicados a ellos.

Detalles de los permisos

Esta política incluye los siguientes permisos:

- `ecr:` permite a las entidades de seguridad leer y escribir en los repositorios, así como leer políticas de ciclo de vida. Las entidades de servicio no tienen permiso para eliminar repositorios o cambiar las políticas de ciclo de vida que se les aplican.

La política AmazonEC2ContainerRegistryPowerUser es como sigue.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",

```

```

        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
        "ecr:BatchGetImage",
        "ecr:GetLifecyclePolicy",
        "ecr:GetLifecyclePolicyPreview",
        "ecr:ListTagsForResource",
        "ecr:DescribeImageScanFindings",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:PutImage"
    ],
    "Resource": "*"
}
]
}

```

AmazonEC2ContainerRegistryReadOnly

Puede adjuntar la política AmazonEC2ContainerRegistryReadOnly a las identidades de IAM.

Esta política otorga permisos de solo lectura a Amazon ECR. Esto incluye la capacidad de mostrar una lista de repositorios e imágenes en los repositorios. También incluye la capacidad de extraer imágenes de Amazon ECR con la CLI de Docker.

Detalles de los permisos

Esta política incluye los siguientes permisos:

- `ecr`: permite a las entidades de seguridad leer repositorios y sus respectivas políticas de ciclo de vida.

La política AmazonEC2ContainerRegistryReadOnly es como sigue.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecr:GetAuthorizationToken",

```

```

        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
        "ecr:BatchGetImage",
        "ecr:GetLifecyclePolicy",
        "ecr:GetLifecyclePolicyPreview",
        "ecr:ListTagsForResource",
        "ecr:DescribeImageScanFindings"
    ],
    "Resource": "*"
}
]
}

```

AWSECRPullThroughCache_ServiceRolePolicy

No puede adjuntar la política de IAM administrada

AWSECRPullThroughCache_ServiceRolePolicy a sus entidades de IAM. Esta política se adjunta a un rol vinculado a servicios que permite a Amazon ECR enviar imágenes a los repositorios a través del flujo de trabajo de extracción de caché. Para obtener más información, consulte [Rol vinculado a servicios de Amazon ECR para la caché de extracción](#).

ECRReplicationServiceRolePolicy

No puede adjuntar la política de IAM administrada ECRReplicationServiceRolePolicy a sus entidades de IAM. Esta política se encuentra adjunta a un rol vinculado a un servicio que permite a Amazon ECR realizar acciones en su nombre. Para obtener más información, consulte [Uso de roles vinculados a servicios para Amazon ECR](#).

Amazon ECR actualiza las políticas AWS gestionadas

Consulte los detalles sobre las actualizaciones de las políticas AWS gestionadas de Amazon ECR desde el momento en que este servicio comenzó a realizar el seguimiento de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbese a la fuente RSS en la página de historial de documentos de Amazon ECR.

Cambio	Descripción	Fecha
<p>AWSECRPullThroughCache_ServiceRolePolicy: actualización de una política actual</p>	<p>Amazon ECR agregó nuevos permisos a la política <code>AWSECRPullThroughCache_ServiceRolePolicy</code>. Estos permisos permiten a Amazon ECR recuperar el contenido cifrado de un secreto de Secrets Manager. Esto es necesario cuando se utiliza una regla de caché de extracción para almacenar en caché las imágenes de un registro anterior que requiere autenticación.</p>	<p>15 de noviembre de 2023</p>
<p>AWSECRPullThroughCache_ServiceRolePolicy: política nueva</p>	<p>Amazon ECR agregó una política nueva. Esta política está asociada con el rol vinculado a servicios <code>AWSServiceRoleForECRPullThroughCache</code> para la característica de extracción de caché.</p>	<p>29 de noviembre de 2021</p>
<p>ECR ReplicationServiceRolePolicy: nueva política</p>	<p>Amazon ECR agregó una política nueva. Esta política está asociada con el rol vinculado a servicios <code>AWSServiceRoleForECRReplication</code> para la característica de replicación.</p>	<p>4 de diciembre de 2020</p>

Cambio	Descripción	Fecha
AmazonEC2 Container Registry FullAccess : actualización a una política existente	Amazon ECR agregó nuevos permisos a la política <code>AmazonEC2ContainerRegistryFullAccess</code> . Estos permisos permiten que las entidades de seguridad creen el rol vinculado al servicio de Amazon ECR.	4 de diciembre de 2020
AmazonEC2 Container Registry ReadOnly : actualización a una política existente	Amazon ECR agregó nuevos permisos a la política <code>AmazonEC2ContainerRegistryReadOnly</code> que permite a las entidades de seguridad leer políticas del ciclo de vida, mostrar una lista de etiquetas y describir los resultados del escaneo para las imágenes.	10 de diciembre de 2019
AmazonEC2 Container Registry PowerUser : actualización a una política existente	Amazon ECR agregó nuevos permisos a la política <code>AmazonEC2ContainerRegistryPowerUser</code> . Estos permiten a las entidades de seguridad leer políticas del ciclo de vida, mostrar una lista de etiquetas y describir los resultados del escaneo para las imágenes.	10 de diciembre de 2019

Cambio	Descripción	Fecha
AmazonEC2 Container Registry FullAccess : actualización a una política existente	Amazon ECR agregó nuevos permisos a la política AmazonEC2ContainerRegistryFullAccess . Permiten a los directores buscar los eventos de administración o los eventos de AWS CloudTrail Insights capturados por. CloudTrail	10 de noviembre de 2017
AmazonEC2 Container Registry ReadOnly : actualización de una política existente	Amazon ECR agregó nuevos permisos a la política AmazonEC2ContainerRegistryReadOnly . Permiten a las entidades de seguridad describir imágenes de Amazon ECR.	11 de octubre de 2016
AmazonEC2 Container Registry PowerUser : actualización a una política existente	Amazon ECR agregó nuevos permisos a la política AmazonEC2ContainerRegistryPowerUser . Permiten a las entidades de seguridad describir imágenes de Amazon ECR.	11 de octubre de 2016

Cambio	Descripción	Fecha
AmazonEC2 Container Registry ReadOnly : nueva política	Amazon ECR ha agregado una política nueva que concede permisos de solo lectura a Amazon ECR. Estos incluyen la capacidad de mostrar una lista de repositorios e imágenes en los repositorios. También incluyen la capacidad de extraer imágenes de Amazon ECR con la CLI de Docker.	21 de diciembre de 2015
AmazonEC2 Container Registry PowerUser : nueva política	Amazon ECR agregó una política nueva que otorga permisos administrativos que permiten que los usuarios lean y escriban en los repositorios, pero no les permite eliminar los repositorios ni cambiar los documentos de la política aplicados a ellos.	21 de diciembre de 2015
AmazonEC2 Container Registry FullAccess : nueva política	Amazon ECR agregó una política nueva. Esta política otorga acceso completo a Amazon ECR.	21 de diciembre de 2015
Amazon ECR comenzó a realizar el seguimiento de los cambios	Amazon ECR comenzó a realizar un seguimiento de los cambios en las políticas AWS gestionadas.	24 de junio de 2021

Uso de roles vinculados a servicios para Amazon ECR

Amazon Elastic Container Registry (Amazon ECR) AWS Identity and Access Management utiliza funciones [vinculadas a servicios \(IAM\)](#) para proporcionar los permisos necesarios para utilizar las funciones de replicación y extracción de memoria caché. Un rol vinculado a un servicio es un tipo único de rol de IAM que se encuentra vinculado directamente a Amazon ECR. Amazon ECR predefine el rol vinculado a un servicio. Incluye todos los permisos que el servicio requiere para respaldar la replicación y las características de caché de su registro privado. Después de configurar la replicación o la extracción de caché de su registro, se crea automáticamente un rol vinculado a servicios en su nombre. Para obtener más información, consulte [Configuración de registro privado en Amazon ECR](#).

Un rol vinculado a servicios facilita la configuración de la replicación y la extracción de caché con Amazon ECR. Esto se debe a que, al usarlo, no tendrá que agregar manualmente todos los permisos necesarios. Amazon ECR define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo Amazon ECR puede asumir sus roles. Los permisos definidos incluyen la política de confianza y la política de permisos. La política de permisos no se puede adjuntar a ninguna otra entidad de IAM.

Puede eliminar el rol vinculado a servicios correspondiente solo después de desactivar la replicación o la extracción de caché en su registro. Esto garantiza que no elimine inadvertidamente los permisos que Amazon ECR requiere para estas características.

Para obtener más información sobre otros servicios que admiten los roles vinculados a servicios, consulte [Servicios de AWS que funcionan con IAM](#). En esta página vinculada, busque los servicios para los que se indique Sí en la columna Roles vinculados a servicios. Elija una opción Sí con un enlace para ver la documentación relevante acerca del rol vinculado al servicio en cuestión.

Temas

- [Regiones admitidas para los roles vinculados a servicios de Amazon ECR](#)
- [Rol vinculado a servicios de Amazon ECR para replicación](#)
- [Rol vinculado a servicios de Amazon ECR para la caché de extracción](#)

Regiones admitidas para los roles vinculados a servicios de Amazon ECR

Amazon ECR admite el uso de roles vinculados a servicios en todas las regiones en las que se encuentra disponible el servicio Amazon ECR. Para obtener más información acerca de la disponibilidad de la región de Amazon ECR, consulte [Regiones y puntos de conexión de AWS](#).

Rol vinculado a servicios de Amazon ECR para replicación

Amazon ECR utiliza un rol vinculado a un servicio denominado que `AWSServiceRoleForECRReplication` permite a Amazon ECR replicar imágenes en varias cuentas.

Permisos de roles vinculados a servicios para Amazon ECR

El rol `AWSServiceRoleForECRReplication` vinculado al servicio confía en los siguientes servicios para asumir el rol:

- `replication.ecr.amazonaws.com`

La siguiente política de permisos del rol `ECRReplicationServiceRolePolicy` permite que Amazon ECR use las siguientes acciones en los recursos:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecr:CreateRepository",
        "ecr:ReplicateImage"
      ],
      "Resource": "*"
    }
  ]
}
```

Note

`ReplicateImage` es una API interna que Amazon ECR utiliza para la replicación y a la que no se puede llamar directamente.

Debe configurar permisos para permitir a una entidad de IAM (como, por ejemplo, un usuario, grupo o rol) crear, editar o eliminar la descripción de un rol vinculado a un servicio. Para obtener más información, consulte [Permisos de roles vinculados a servicios](#) en la Guía del usuario de IAM.

Creación de un rol vinculado a un servicio para Amazon ECR

No necesita crear manualmente el rol vinculado al servicio de Amazon ECR. Al configurar los ajustes de replicación para su registro en la AWS Management Console, AWS CLI, la o la AWS API, Amazon ECR crea automáticamente la función vinculada al servicio.

Si elimina este rol vinculado a un servicio y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al configurar los parámetros de replicación para el registro, Amazon ECR crea automáticamente el rol vinculado a un servicio otra vez.

Edición de un rol vinculado a un servicio para Amazon ECR

Amazon ECR no permite editar manualmente el rol vinculado al `AWSServiceRoleForECRReplication` servicio. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte [Editar un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Eliminación de un rol vinculado a un servicio para Amazon ECR

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a servicios, recomendamos que elimine dicho rol. De esta forma no conservará una entidad no utilizada que no se monitorice ni se mantenga de forma activa. No obstante, debe quitar la configuración de replicación del registro en cada región para poder eliminar manualmente el rol vinculado a un servicio.

Note

Si intenta eliminar recursos mientras el servicio Amazon ECR sigue utilizando los roles, es posible que la acción de eliminación falle. Si eso sucede, espere unos minutos e inténtelo de nuevo.

Para eliminar los recursos de Amazon ECR utilizados por el `AWSServiceRoleForECRReplication`

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/>.
2. En la barra de navegación, elija la región en la que está establecida la configuración de replicación.
3. En el panel de navegación, elija Private registry (Registro privado).

4. En la página Private registry (Registro privado), en la sección Replication configuration (Configuración de replicación), elija Edit (Editar).
5. Para eliminar todas las reglas de replicación, elija Delete all (Eliminar todo). Este paso requiere confirmación.

Eliminación manual del rol vinculado a servicios mediante IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al `AWSServiceRoleForECRReplicationservicio`. Para más información, consulte [Eliminación de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Rol vinculado a servicios de Amazon ECR para la caché de extracción

Amazon ECR utiliza un rol vinculado a un servicio denominado `AWSServiceRoleForECRPullThroughCache` que permite a Amazon ECR realizar acciones en su nombre para completar las acciones de extracción de caché. Para obtener más información acerca de la caché de extracción, consulte [Sincronice un registro anterior con un registro privado de Amazon ECR](#).

Permisos de roles vinculados a servicios para Amazon ECR

El rol `AWSServiceRoleForECRPullThroughCache` vinculado al servicio confía en que el siguiente servicio asuma el rol.

- `pullthroughcache.ecr.amazonaws.com`

Detalles de los permisos

La política de permisos `AWSECRPullThroughCache_ServiceRolePolicy` se adjunta al rol vinculado al servicio. Esta política administrada otorga a Amazon ECR permiso para realizar las siguientes acciones. Para obtener más información, consulte [AWSECRPullThroughCache_ServiceRolePolicy](#).

- `ecr`: permite que el servicio Amazon ECR envíe imágenes a un repositorio privado.
- `secretsmanager:GetSecretValue`— Permite que el servicio Amazon ECR recupere el contenido cifrado de un AWS Secrets Manager secreto. Esto es necesario cuando se utiliza una regla de caché de extracción para almacenar en caché las imágenes de un registro anterior que requiere autenticación en un registro privado. Este permiso solo se aplica a los secretos con el prefijo de nombre `ecr-pullthroughcache/`.

La política `AWSECRPullThroughCache_ServiceRolePolicy` contiene los siguientes JSON.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ECR",
      "Effect": "Allow",
      "Action": [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:PutImage"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SecretsManager",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": "arn:aws:secretsmanager:*:*:secret:ecr-pullthroughcache/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Debe configurar permisos para permitir a una entidad de IAM (como, por ejemplo, un usuario, grupo o rol) crear, editar o eliminar la descripción de un rol vinculado a un servicio. Para obtener más información, consulte [Permisos de roles vinculados a servicios](#) en la Guía del usuario de IAM.

Creación de un rol vinculado a un servicio para Amazon ECR

No es necesario crear manualmente el rol vinculado a servicios de Amazon ECR para la extracción de caché. Cuando crea una regla de extracción de caché para su registro privado en la AWS

Management Console, la AWS CLI o la AWS API, Amazon ECR crea automáticamente la función vinculada al servicio.

Si elimina este rol vinculado a un servicio y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando crea una regla de caché de extracción para su registro privado, Amazon ECR crea el rol vinculado a servicios nuevamente para usted si aún no existe.

Edición de un rol vinculado a un servicio para Amazon ECR

Amazon ECR no permite editar manualmente el rol vinculado al `AWSServiceRoleForECRPullThroughCache` servicio. Una vez creado el rol vinculado a servicios, no puede cambiar el nombre del rol porque varias entidades pueden hacer referencia a este. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte [Editar un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Eliminación de un rol vinculado a un servicio para Amazon ECR

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a servicios, recomendamos que elimine dicho rol. De esta forma no conservará una entidad no utilizada que no se monitorice ni se mantenga de forma activa. No obstante, debe eliminar las reglas de caché de extracción para su registro en cada región antes de poder eliminar manualmente el rol vinculado a servicios.

Note

Si intenta eliminar recursos mientras el servicio Amazon ECR sigue utilizando el rol, es posible que la acción de eliminación falle. Si eso sucede, espere unos minutos e inténtelo de nuevo.

Para eliminar los recursos de Amazon ECR utilizados por el rol vinculado a servicios `AWSServiceRoleForECRPullThroughCache`:

1. Abra la consola de Amazon ECR en <https://console.aws.amazon.com/ecr/>.
2. En la barra de navegación, elija la región donde se crean las reglas de caché de extracción.
3. En el panel de navegación, elija Private registry (Registro privado).
4. En la página Private registry (Registro privado), en la sección Pull through cache configuration (Configuración de la caché de extracción), elija Edit (Editar).

5. Para cada regla de caché de extracción que haya creado, seleccione la regla y, a continuación, elija Delete rule (Eliminar regla).

Eliminación manual del rol vinculado a servicios mediante IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al servicio. `AWSServiceRoleForECRPullThroughCache` Para más información, consulte [Eliminación de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Solución de problemas de identidad y acceso para Amazon Elastic Container Registry

Utilice la siguiente información para diagnosticar y solucionar los problemas habituales que es posible que surjan cuando se trabaja con Amazon ECR e IAM.

Temas

- [No tengo autorización para realizar una acción en Amazon ECR](#)
- [No estoy autorizado a realizar lo siguiente: PassRole](#)
- [Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Amazon ECR](#)

No tengo autorización para realizar una acción en Amazon ECR

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio `my-example-widget`, pero no tiene los permisos ficticios `ecr:GetWidget`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
ecr:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso `my-example-widget` mediante la acción `ecr:GetWidget`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar lo siguiente: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, sus políticas deben actualizarse a fin de permitirle pasar un rol a Amazon ECR.

Algunos Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Amazon ECR. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Amazon ECR

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para saber si Amazon ECR admite estas características, consulte [Cómo funciona Amazon Elastic Container Registry con IAM](#).
- Para obtener información sobre cómo proporcionar acceso a sus recursos a través de los Cuentas de AWS que posee, consulte [Proporcionar acceso a un usuario de IAM en otro de su propiedad Cuenta de AWS en la Guía del usuario de IAM](#).

- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta [Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros](#) en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte [Proporcionar acceso a usuarios autenticados externamente \(identidad federada\)](#) en la Guía del usuario de IAM.
- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte [Cómo los roles de IAM difieren de las políticas basadas en recursos](#) en la Guía del usuario de IAM.

Protección de los datos en Amazon ECR

El [modelo de](#) se aplica a protección de datos en Amazon Elastic Container Service. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las [Preguntas frecuentes sobre la privacidad de datos](#). Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el [Modelo de responsabilidad compartida de AWS y GDPR](#) en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.

- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte [Estándar de procesamiento de la información federal \(FIPS\) 140-2](#).

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con Amazon ECS u otro dispositivo Servicios de AWS mediante la consola, la API o AWS los SDK. AWS CLI Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya la información de las credenciales en la URL para validar la solicitud para ese servidor.

Temas

- [Cifrado en reposo](#)

Cifrado en reposo

Amazon ECR almacena imágenes en depósitos de Amazon S3 que administra Amazon ECR. De forma predeterminada, Amazon ECR utiliza el cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 que cifran los datos en reposo mediante un algoritmo de cifrado AES-256. Esto no requiere ninguna acción por su parte y no conlleva ningún cargo adicional. Para obtener más información, consulte [Protecting Data Using Server-Side Encryption with Amazon S3-Managed Encryption Keys \(SSE-S3\)](#) (Protección de datos mediante el cifrado que se ejecuta en el servidor con las claves de cifrado administradas por Amazon S3 [SSE-S3]) en la Guía del usuario de Amazon Simple Storage Service.

Para tener más control sobre el cifrado de sus repositorios de Amazon ECR, puede utilizar el cifrado del lado del servidor con claves de KMS almacenadas en (). AWS Key Management Service AWS KMS Al cifrar AWS KMS los datos, puede utilizar la predeterminada, que gestiona Amazon ECR Clave administrada de AWS, o especificar su propia clave de KMS (denominada clave gestionada por el cliente). Para obtener más información, consulte [Protección de datos mediante el cifrado del lado del servidor con claves de KMS almacenadas en AWS KMS \(SSE-KMS\)](#) en la Guía del usuario de Amazon Simple Storage Service.

Cada repositorio de Amazon ECR tiene una configuración de cifrado, que se establece cuando este se crea. En cada repositorio se pueden utilizar diferentes configuraciones de cifrado. Para obtener más información, consulte [Creación de un repositorio privado de Amazon ECR para almacenar imágenes](#).

Cuando se crea un repositorio con el AWS KMS cifrado activado, se utiliza una clave KMS para cifrar el contenido del repositorio. Además, Amazon ECR añade una AWS KMS concesión a la clave de KMS con el repositorio Amazon ECR como principal beneficiario.

A continuación se proporciona una descripción de alto nivel sobre cómo Amazon ECR se integra con AWS KMS para cifrar y descifrar sus repositorios:

1. Al crear un repositorio, Amazon ECR envía una [DescribeKey](#) llamada AWS KMS a para validar y recuperar el nombre de recurso de Amazon (ARN) de la clave de KMS especificada en la configuración de cifrado.
2. Amazon ECR envía dos [CreateGrant](#) solicitudes AWS KMS para crear concesiones en la clave de KMS para que Amazon ECR pueda cifrar y descifrar datos mediante la clave de datos.
3. Al insertar una imagen, se solicita una [GenerateDataclave](#) AWS KMS que especifica la clave KMS que se utilizará para cifrar la capa de imágenes y el manifiesto.
4. AWS KMS genera una nueva clave de datos, la cifra con la clave KMS especificada y envía la clave de datos cifrada para que se almacene junto con los metadatos de la capa de imágenes y el manifiesto de la imagen.
5. Al extraer una imagen, se envía una solicitud de [descifrado](#) AWS KMS, especificando la clave de datos cifrados.
6. AWS KMS descifra la clave de datos cifrada y la envía a Amazon S3.
7. La clave de datos se utiliza para descifrar la capa de imagen antes de que esta se extraiga.
8. Cuando se elimina un repositorio, Amazon ECR envía dos [RetireGrants](#) solicitudes AWS KMS para retirar las concesiones creadas para el repositorio.

Consideraciones

Se deben tener en cuenta los siguientes puntos al utilizar el AWS KMS cifrado con Amazon ECR.

- Si crea su repositorio de Amazon ECR con cifrado de KMS y no especifica una clave de KMS, Amazon ECR utiliza una Clave administrada de AWS con el alias de forma `aws/ecr` predeterminada. Esta clave KMS se crea en su cuenta la primera vez que crea un repositorio con cifrado KMS habilitado.

- Cuando utiliza el cifrado KMS con su propia clave KMS, la clave debe existir en la misma región que el repositorio.
- No se deben revocar las concesiones que Amazon ECR crea en su nombre. Si revoca la autorización que autoriza a Amazon ECR a utilizar las AWS KMS claves de su cuenta, Amazon ECR no podrá acceder a estos datos, cifrar las nuevas imágenes introducidas en el repositorio ni descifrarlas cuando se extraigan. Al revocar una concesión para Amazon ECR, el cambio se produce inmediatamente. Para revocar derechos de acceso, debe eliminar el repositorio en lugar de revocar la concesión. Cuando se elimina un repositorio, Amazon ECR retira las concesiones en su nombre.
- El uso de las claves conlleva un coste. AWS KMS Para más información, consulte [Precios de AWS Key Management Service](#).

Permisos de IAM necesarios

Al crear o eliminar un repositorio de Amazon ECR con cifrado del lado del servidor mediante AWS KMS, los permisos necesarios dependen de la clave KMS específica utilice.

Permisos de IAM necesarios cuando se utiliza Clave administrada de AWS para Amazon ECR

De forma predeterminada, cuando el AWS KMS cifrado está habilitado para un repositorio de Amazon ECR pero no se especifica ninguna clave de KMS, se utiliza la Clave administrada de AWS de Amazon ECR. Cuando la clave AWS de KMS administrada para Amazon ECR se usa para cifrar un repositorio, cualquier responsable que tenga permiso para crear un repositorio también puede habilitar el AWS KMS cifrado en el repositorio. No obstante, la entidad de seguridad de IAM que elimina el repositorio debe tener el permiso `kms:RetireGrant`. Esto permite retirar las concesiones que se agregaron a la AWS KMS clave cuando se creó el repositorio.

El siguiente ejemplo de política de IAM se puede agregar como política insertada a un usuario para asegurarse de que tiene los permisos mínimos necesarios para eliminar un repositorio que tenga habilitado el cifrado. La clave KMS utilizada para cifrar el repositorio se puede especificar mediante el parámetro de recurso.

```
{
  "Version": "2012-10-17",
  "Id": "ecr-kms-permissions",
  "Statement": [
    {
      "Sid": "AllowAccessToRetireTheGrantsAssociatedWithTheKey",
```

```

        "Effect": "Allow",
        "Action": [
            "kms:RetireGrant"
        ],
        "Resource": "arn:aws:kms:us-
west-2:111122223333:key/b8d9ae76-080c-4043-92EXAMPLE"
    }
]
}

```

Permisos de IAM necesarios cuando se utiliza una clave administrada por el cliente

Al crear un repositorio con el AWS KMS cifrado habilitado mediante una clave administrada por el cliente, se requieren permisos tanto para la política de claves de KMS como para la política de IAM para el usuario o rol que crea el repositorio.

Al crear su propia clave KMS, puede usar la política de clave AWS KMS predeterminada o especificar la suya propia. Para garantizar que el propietario de la cuenta siga siendo administrable por el propietario de la cuenta, la política de claves de la clave de KMS debe permitir todas AWS KMS las acciones del usuario raíz de la cuenta. Es posible que se agreguen permisos de ámbito adicionales a la política de clave, pero como mínimo se le deben dar permisos al usuario raíz para administrar la clave KMS. Para permitir que la clave KMS se use solo para las solicitudes que se originan en Amazon ECR, puede usar la [clave de ViaService condición kms:](#) con el `ecr.<region>.amazonaws.com` valor.

El siguiente ejemplo de política de claves otorga a la AWS cuenta (usuario raíz) propietaria de la clave de KMS acceso total a la clave de KMS. Para obtener más información sobre este ejemplo de política clave, consulte Permitir [el acceso a la AWS cuenta y Habilitar las políticas de IAM](#) en la Guía para AWS Key Management Service desarrolladores.

```

{
  "Version": "2012-10-17",
  "Id": "ecr-key-policy",
  "Statement": [
    {
      "Sid": "EnableIAMUserPermissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "kms:*",

```

```

        "Resource": "*"
    }
]
}

```

El usuario de IAM, el rol de IAM o la AWS cuenta que crea los repositorios debe tener el `kms:DescribeKey` permiso y `kms:CreateGrant``kms:RetireGrant`, además de los permisos de Amazon ECR necesarios.

Note

El permiso `kms:RetireGrant` se debe agregar a la política de IAM del usuario o rol que crea el repositorio. Los permisos `kms:CreateGrant` y `kms:DescribeKey` se pueden agregar a la política de clave para la clave KMS, o a la política de IAM del usuario o rol que crea el repositorio. Para obtener más información sobre cómo funcionan AWS KMS los permisos, consulte la [referencia sobre permisos de AWS KMS API: acciones y recursos](#) en la Guía para desarrolladores.AWS Key Management Service

El siguiente ejemplo de política de IAM se puede agregar como política insertada a un usuario, para asegurarse de que tiene los permisos mínimos necesarios para crear un repositorio que tenga habilitado el cifrado y borrarlo cuando haya terminado de utilizarlo. La AWS KMS key utilizada para cifrar el repositorio se puede especificar mediante el parámetro de recurso.

```

{
  "Version": "2012-10-17",
  "Id": "ecr-kms-permissions",
  "Statement": [
    {
      "Sid":
"AllowAccessToCreateAndRetireTheGrantsAssociatedWithTheKeyAsWellAsDescribeTheKey",
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:RetireGrant",
        "kms:DescribeKey"
      ],
      "Resource": "arn:aws:kms:us-
west-2:111122223333:key/b8d9ae76-080c-4043-92EXAMPLE"
    }
  ]
}

```

```
]
}
```

Habilitación de un usuario para mostrar una lista de claves KMS en la consola al crear un repositorio

Cuando utilice la consola de Amazon ECR para crear un repositorio, puede conceder permisos para permitir que un usuario publique las claves KMS administradas por el cliente en la región al habilitar el cifrado para el repositorio. En el siguiente ejemplo de política de IAM se muestran los permisos necesarios para mostrar una lista de las claves KMS y alias cuando se utiliza la consola.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:ListKeys",
      "kms:ListAliases",
      "kms:DescribeKey"
    ],
    "Resource": "*"
  }
}
```

Monitoreo de la interacción de Amazon ECR con AWS KMS

Puede utilizarlo AWS CloudTrail para realizar un seguimiento de las solicitudes que Amazon ECR envía AWS KMS en su nombre. Las entradas de registro del CloudTrail registro contienen una clave de contexto de cifrado para que sean más fáciles de identificar.

Contexto de cifrado de Amazon ECR

Un contexto de cifrado es un conjunto de pares de clave-valor que contiene datos no secretos arbitrarios. Al incluir un contexto de cifrado en una solicitud de cifrado de datos, vincula AWS KMS criptográficamente el contexto de cifrado a los datos cifrados. Para descifrar los datos, es necesario pasar el mismo contexto de cifrado.

En sus solicitudes de [GenerateDataclave](#) y [descifrado](#) AWS KMS, Amazon ECR utiliza un contexto de cifrado con dos pares de nombre-valor que identifican el repositorio y el bucket de Amazon S3 que se está utilizando. Esto se muestra en el siguiente ejemplo. Los nombres no varían, pero los valores de contexto de cifrado combinado serán diferentes para cada valor.

```
"encryptionContext": {
  "aws:s3:arn": "arn:aws:s3::us-west-2-starport-manifest-bucket/EXAMPLE1-90ab-cdef-fedc-ba987BUCKET1/sha256:a7766145a775d39e53a713c75b6fd6d318740e70327aaa3ed5d09e0ef33fc3df",
  "aws:ecr:arn": "arn:aws:ecr:us-west-2:111122223333:repository/repository-name"
}
```

Puede usar el contexto de cifrado para identificar estas operaciones criptográficas en registros y registros de auditoría, como [AWS CloudTrail](#) Amazon CloudWatch Logs, y como condición para la autorización en políticas y concesiones.

El contexto de cifrado de Amazon ECR se compone de dos pares de nombre-valor.

- `aws:s3:arn`: el primer par de nombre-valor identifica el bucket. La clave es `aws:s3:arn`. El valor es el Nombre de recurso de Amazon (ARN) del bucket de Amazon S3.

```
"aws:s3:arn": "ARN of an Amazon S3 bucket"
```

Por ejemplo, si el ARN del bucket fuera `arn:aws:s3::us-west-2-starport-manifest-bucket/EXAMPLE1-90ab-cdef-fedc-ba987BUCKET1/sha256:a7766145a775d39e53a713c75b6fd6d318740e70327aaa3ed5d09e0ef33fc3df`, el contexto de cifrado incluiría el siguiente par.

```
"arn:aws:s3::us-west-2-starport-manifest-bucket/EXAMPLE1-90ab-cdef-fedc-ba987BUCKET1/sha256:a7766145a775d39e53a713c75b6fd6d318740e70327aaa3ed5d09e0ef33fc3df"
```

- `aws:ecr:arn`: el segundo par de nombre-valor identifica el Nombre de recurso de Amazon (ARN) del repositorio. La clave es `aws:ecr:arn`. El valor representa el ARN del proyecto.

```
"aws:ecr:arn": "ARN of an Amazon ECR repository"
```

Por ejemplo, si el ARN del repositorio fuera `arn:aws:ecr:us-west-2:111122223333:repository/repository-name`, el contexto de cifrado incluiría el siguiente par.

```
"aws:ecr:arn": "arn:aws:ecr:us-west-2:111122223333:repository/repository-name"
```

Resolución de problemas

Al eliminar un repositorio de Amazon ECR con la consola, si el repositorio se elimina correctamente pero Amazon ECR no puede retirar las concesiones agregadas a la clave KMS para su repositorio, recibirá el siguiente error.

```
The repository [{repository-name}] has been deleted successfully but the grants created by the kmsKey [{kms_key}] failed to be retired
```

Cuando esto ocurra, podrá retirar usted mismo las AWS KMS subvenciones para el repositorio.

Para retirar manualmente AWS KMS las subvenciones para un repositorio

1. Enumere las concesiones para la AWS KMS clave utilizada para el repositorio. El valor `key-id` se incluye en el error que recibe de la consola. También puede usar el `list-keys` comando para enumerar las claves de KMS Claves administradas por AWS y las administradas por el cliente en una región específica de su cuenta.

```
aws kms list-grants \  
  --key-id b8d9ae76-080c-4043-9237-c815bfc21dfc \  
  --region us-west-2
```

La salida incluye un elemento `EncryptionContextSubset` con el Nombre de recurso de Amazon (ARN) del repositorio. Esto se puede utilizar para determinar qué concesión agregada a la clave es la que desea retirar. En el siguiente paso se usará el valor `GrantId` al retirar la concesión.

2. Retira cada concesión de la AWS KMS clave agregada al repositorio. Sustituya el valor `for` por *GrantId* del ID de la concesión del resultado del paso anterior.

```
aws kms retire-grant \  
  --key-id b8d9ae76-080c-4043-9237-c815bfc21dfc \  
  --grant-id GrantId \  
  --region us-west-2
```

Validación de conformidad para Amazon Elastic Container Registry


Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte [Servicios de AWS Alcance por programa de cumplimiento](#)

[Servicios de AWS](#) de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de [AWS cumplimiento > Programas AWS](#) .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte [Descarga de informes en AWS Artifact](#) .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- [Guías de inicio rápido sobre seguridad y cumplimiento](#): estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseño de [arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services](#): en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

 Note

No Servicios de AWS todas cumplen los requisitos de la HIPAA. Para más información, consulte la [Referencia de servicios compatibles con HIPAA](#).

- [AWS Recursos de](#) cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- [AWS Guías de cumplimiento para clientes](#): comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- [Evaluación de los recursos con reglas](#) en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- [AWS Security Hub](#)— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la [Referencia de controles de Security Hub](#).

- [Amazon GuardDuty](#): Servicio de AWS detecta posibles amenazas para sus cargas de trabajo. Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- [AWS Audit Manager](#)— Este Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Seguridad de la infraestructura en Amazon Elastic Container Registry

Como servicio gestionado, Amazon Elastic Container Registry está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte [Seguridad AWS en la nube](#). Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte [Protección de infraestructuras en un marco](#) de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a Amazon ECR a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM principal. También puede utilizar [AWS Security Token Service](#) (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Puede llamar a estas operaciones de la API desde cualquier ubicación de red, pero Amazon ECR admite políticas de acceso basadas en recursos, que pueden incluir restricciones en función de la dirección IP de origen. También puede utilizar políticas de Amazon ECR para controlar el acceso desde puntos de enlace específicos de Amazon Virtual Private Cloud (Amazon VPC) o VPC específicas. En efecto, esto aísla el acceso a la red a un recurso de Amazon ECR determinado

únicamente de la VPC específica de la red. AWS Para obtener más información, consulte [Puntos de enlace de VPC de la interfaz Amazon ECR \(AWS PrivateLink\)](#).

Puntos de enlace de VPC de la interfaz Amazon ECR (AWS PrivateLink)

Para mejorar la posición de seguridad de su VPC, configure Amazon ECR para que utilice un punto de enlace de la VPC de tipo interfaz. Los puntos de enlace de VPC funcionan con una tecnología que le permite acceder de forma privada a las API de Amazon ECR a través de direcciones IP privadas. AWS PrivateLink AWS PrivateLink restringe todo el tráfico de red entre la VPC y Amazon ECR a la red de Amazon. No necesita una gateway de Internet, un dispositivo NAT ni una gateway privada virtual.

Para obtener más información sobre AWS PrivateLink los puntos de enlace de VPC, consulte los puntos de enlace de [VPC en la Guía del usuario](#) de Amazon VPC.

Consideraciones para los puntos de enlace de la VPC de Amazon ECR

Antes de configurar los puntos de enlace de la VPC para Amazon ECR, debe tener en cuenta las consideraciones siguientes.

- Para permitir que las tareas de Amazon ECS alojadas en instancias de Amazon EC2 extraigan imágenes privadas de Amazon ECR, asegúrese de crear también los puntos de enlace de la VPC de tipo interfaz para Amazon ECS. Para obtener más información, consulte [Interface VPC Endpoints \(AWS PrivateLink\)](#) en la Guía para desarrolladores de Amazon Elastic Container Service.

Important

Las tareas de Amazon ECS alojadas en Fargate no requieren los puntos de enlace de la VPC de tipo interfaz de Amazon ECS.

- Las tareas de Amazon ECS alojadas en Fargate que utilizan la versión 1.3.0 o una anterior de la plataforma de Linux solo requieren el punto de conexión de VPC de Amazon ECR `com.amazonaws.región.ecr.dkr` y el punto de conexión de puerta de enlace de Amazon S3 para aprovechar esta característica.
- Las tareas de Amazon ECS alojadas en Fargate con la versión 1.4.0 o posterior de la plataforma de Linux requieren los puntos de conexión de VPC de Amazon ECR `com.amazonaws.región.ecr.dkr` y `com.amazonaws.región.ecr.api`, así como el punto de conexión de puerta de enlace de Amazon S3, para aprovechar esta característica.

- Las tareas de Amazon ECS alojadas en Fargate con la versión 1.0.0 o posterior de la plataforma de Windows requieren los puntos de conexión de VPC de Amazon ECR `com.amazonaws.region.ecr.dkr` y `com.amazonaws.region.ecr.api` , así como el punto de conexión de puerta de enlace de Amazon S3, para aprovechar esta característica.
- Las tareas de Amazon ECS alojadas en Fargate que extraen imágenes de contenedor de Amazon ECR pueden restringir el acceso a la VPC específica que utilizan las tareas y al punto de enlace de la VPC que utiliza el servicio. Para ello, se agregan claves de condición al rol de IAM de ejecución de tareas para la tarea. Para obtener más información, consulte [Permisos de IAM opcionales para tareas de Fargate que extraen imágenes de Amazon ECR sobre puntos de enlace de interfaz](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- Las tareas de Amazon ECS alojadas en Fargate que extraen imágenes de contenedores de Amazon ECR y que también utilizan el controlador de registro para enviar información de `awslogs` registro a CloudWatch Logs requieren el punto de enlace de CloudWatch VPC de Logs. Para obtener más información, consulte [Cree el punto final de CloudWatch Logs](#).
- El grupo de seguridad asociado al punto de conexión de la VPC debe permitir las conexiones entrantes en el puerto 443 desde la subred privada de la VPC.
- Los puntos de enlace de la VPC no admiten las solicitudes entre regiones. Asegúrese de crear los puntos de enlace de la VPC en la misma región en la que tiene previsto enviar llamadas a la API de Amazon ECR.
- Los puntos de conexión de la VPC actualmente no admiten los repositorios públicos de Amazon ECR. Considere utilizar una regla de caché de extracción para alojar la imagen pública en un repositorio privado en la misma región que el punto de conexión de VPC. Para obtener más información, consulte [Sincronice un registro anterior con un registro privado de Amazon ECR](#).
- Los puntos de enlace de VPC solo admiten el DNS AWS proporcionado a través de Amazon Route 53. Si desea utilizar su propio DNS, puede utilizar el enrutamiento de DNS condicional. Para obtener más información, consulte [Conjuntos de opciones de DHCP](#) en la Guía del usuario de Amazon VPC.
- Si los contenedores tienen conexiones existentes a Amazon S3, sus conexiones podrían interrumpirse brevemente al agregar el punto de enlace de gateway de Amazon S3. Si desea evitar dicha interrupción, cree una nueva VPC que utilice el punto de enlace de gateway de Amazon S3 y luego migre el clúster de Amazon ECS y sus contenedores a la nueva VPC.
- Cuando se extrae una imagen mediante una regla de caché de extracción por primera vez, si ha configurado Amazon ECR para usar un punto de conexión de VPC de interfaz mediante AWS PrivateLink , entonces necesita crear una subred pública en la misma VPC, con una puerta de enlace NAT y, luego, dirigir todo el tráfico saliente a Internet desde su subred privada a la puerta

de enlace NAT para que funcione la extracción. Las extracciones de imágenes posteriores no requieren esto. Para obtener más información, consulte [Escenario: acceso a Internet desde una subred privada](#) en la Guía del usuario de Amazon Virtual Private Cloud.

Consideraciones sobre las imágenes de Windows

Las imágenes basadas en el sistema operativo Windows incluyen artefactos cuya distribución está restringida por licencia. De forma predeterminada, al insertar imágenes de Windows a un repositorio de Amazon ECR, las capas que incluyen estos artefactos no se insertan, ya que se consideran capas externas. Cuando Microsoft proporciona los artefactos, las capas externas se recuperan de la infraestructura de Microsoft Azure. Por este motivo, para habilitar a los contenedores a de modo que puedan extraer estas capas externas de Azure, además de crear los puntos de enlace de la VPC se necesitarán completar más pasos.

Es posible anular este comportamiento al insertar imágenes de Windows a Amazon ECR mediante la marca `--allow-nondistributable-artifacts` en el daemon de Docker. Cuando se habilita, esta marca insertará las capas con licencia a Amazon ECR, lo que permite extraer estas imágenes de Amazon ECR a través del punto de enlace de la VPC sin que se necesite acceso adicional a Azure.

Important

El uso de la marca `--allow-nondistributable-artifacts` no excluye su obligación de cumplir con los términos de la licencia de imagen base de contenedor de Windows; no puede publicar contenido de Windows para redistribución pública o de terceros. Se permite el uso dentro de su propio entorno.

Para habilitar el uso de esta marca para la instalación de Docker, debe modificar el archivo de configuración del daemon de Docker que, en función de la instalación de Docker, normalmente se puede configurar en el menú de configuración o preferencias de la sección Docker Engine (Motor de Docker) o editando el archivo `C:\ProgramData\docker\config\daemon.json` directamente.

A continuación, mostramos un ejemplo de la configuración requerida. Reemplace el valor por el URI del repositorio al que está enviando imágenes.

```
{  
  "allow-nondistributable-artifacts": [  

```

```
"111122223333.dkr.ecr.us-west-2.amazonaws.com"  
]  
}
```

Después de modificar el archivo de configuración del daemon de Docker, debe reiniciar este daemon antes de intentar insertar la imagen. Confirme que la inserción ha funcionado verificando que la capa base se ha integrado con su repositorio.

Note

Las capas base de las imágenes de Windows son grandes. El tamaño de la capa se traducirá en un mayor tiempo de inserción y en que estas imágenes conllevarán costos de almacenamiento adicionales en Amazon ECR. Por estas razones, se recomienda utilizar esta opción únicamente cuando sea estrictamente necesario reducir los tiempos de compilación y los costos de almacenamiento continuos. Por ejemplo, la imagen `mcr.microsoft.com/windows/servercore` tiene un tamaño aproximado de 1,7 GiB cuando se comprime en Amazon ECR.

Creación de puntos de enlace de la VPC para Amazon ECR

Para crear los puntos de enlace de la VPC para el servicio Amazon ECR, utilice el procedimiento [Creación de un punto de enlace de interfaz](#) en la Guía del usuario de Amazon VPC.

Las tareas de Amazon ECS alojadas en instancias de Amazon EC2 requieren los puntos de enlace de Amazon ECR y el punto de enlace de gateway de Amazon S3.

Las tareas de Amazon ECS alojadas en Fargate que utilizan la versión de la plataforma 1.4.0, o una posterior, requieren los puntos de enlace de la VPC de Amazon ECR y los de gateway de Amazon S3.

Las tareas de Amazon ECS alojadas en Fargate que utilizan la versión de la plataforma 1.3.0, o una anterior, solo requieren el punto de enlace de la VPC de Amazon ECR `com.amazonaws.region.ecr.dkr` y los puntos de enlace de gateway de Amazon S3.

Note


El orden en el que se crean los puntos de enlace no importa.

com.amazonaws.*region*.ecr.dkr

Este punto de conexión se utiliza para las API de Docker Registry. Los comandos del cliente de Docker como `push` y `pull` utilizan este punto de conexión.

Al crear este punto de enlace, debe habilitar un nombre de host de DNS privado. Para ello, asegúrese de que la opción `Enable Private DNS Name` (Habilitar nombre de DNS privado) está seleccionada en la consola de Amazon VPC al crear el punto de enlace de la VPC.

com.amazonaws.*region*.ecr.api

 Note

La *región* especificada representa el identificador de región de una AWS región compatible con Amazon ECR, como `us-east-2` la región EE.UU. Este (Ohio).

Este punto de enlace se utiliza para las llamadas a la API de Amazon ECR. Acciones de la API como `DescribeImages` y `CreateRepository` van a este punto de conexión.

Cuando se crea este punto de enlace, tiene la opción de habilitar un nombre de host DNS privado. Habilite esta configuración seleccionando `Enable Private DNS Name` (Habilitar nombre de DNS privado) en la consola de VPC al crear el punto de conexión de la VPC. Si habilitas un nombre de host DNS privado para el punto de conexión de la VPC, actualiza el SDK AWS CLI o a la versión más reciente para que no sea necesario especificar una URL de punto final cuando utilices el SDK AWS CLI .

Si habilitas un nombre de host DNS privado y utilizas un SDK o una AWS CLI versión publicada antes del 24 de enero de 2019, debes usar el `--endpoint-url` parámetro para especificar los puntos finales de la interfaz. En el ejemplo siguiente se muestra el formato de la dirección URL del punto de conexión.

```
aws ecr create-repository --repository-name name --endpoint-url https://  
api.ecr.region.amazonaws.com
```

Si no habilita un nombre de host de DNS privado para el punto de conexión de la VPC, debe utilizar el parámetro `--endpoint-url` que especifique el ID de punto de conexión de la VPC para el punto de conexión de interfaz. En el ejemplo siguiente se muestra el formato de la dirección URL del punto de conexión.

```
aws ecr create-repository --repository-name name --endpoint-url  
https://VPC_endpoint_ID.api.ecr.region.vpce.amazonaws.com
```

Creación del punto de enlace de gateway de Amazon S3

Para que sus tareas de Amazon ECS extraigan imágenes privadas de Amazon ECR, debe crear un punto de enlace de gateway para Amazon S3. El punto de enlace de gateway es necesario porque Amazon ECR utiliza Amazon S3 para almacenar las capas de imágenes. Cuando sus contenedores descargan imágenes de Amazon ECR, deben acceder a Amazon ECR para obtener el manifiesto de imagen y a Amazon S3 para descargar las capas de imágenes en sí. A continuación, se muestra el Nombre de recurso de Amazon (ARN) del bucket de Amazon S3 que contiene las capas para cada imagen de Docker.

```
arn:aws:s3:::prod-region-starport-layer-bucket/*
```

Use el procedimiento [Creación de un punto de enlace de gateway](#) en la Guía del usuario de Amazon VPC para crear el siguiente punto de enlace de gateway de Amazon S3 para Amazon ECR. Cuando cree el punto de conexión, asegúrese de seleccionar las tablas de enrutamiento para su VPC.

com.amazonaws.*region*.s3

El punto de enlace de gateway de Amazon S3 utiliza un documento de políticas de IAM para limitar el acceso al servicio. Se puede utilizar la política de Acceso completo, porque cualquier restricción que haya incluido en los roles de IAM de la tarea u otras políticas de usuario de IAM tienen vigencia sobre esta política. Si quiere limitar el acceso al bucket de Amazon S3 a los permisos mínimos necesarios para utilizar Amazon ECR, consulte [Permisos mínimos del bucket de Amazon S3 para Amazon ECR](#).

Permisos mínimos del bucket de Amazon S3 para Amazon ECR

El punto de enlace de gateway de Amazon S3 utiliza un documento de políticas de IAM para limitar el acceso al servicio. Para permitir solo los permisos mínimos del bucket de Amazon S3 para Amazon ECR, restrinja el acceso al bucket de Amazon S3 que utiliza Amazon ECR al crear el documento de política de IAM para el punto de enlace.

En la siguiente tabla se describen los permisos de política de buckets de Amazon S3 necesarios para Amazon ECR.

Permiso	Descripción
<code>arn:aws:s3:::prod-<i>region</i>-starport-layer-bucket/*</code>	Proporciona acceso al bucket de Amazon S3 que contiene las capas para cada imagen de Docker. Representa el identificador de región de una región de AWS compatible con Amazon ECR, como lo es <code>us-east-2</code> para Este de EE. UU. (Ohio).

Ejemplo

El siguiente ejemplo ilustra cómo proporcionar acceso a los buckets de Amazon S3 necesarios para las operaciones de Amazon ECR.

```
{
  "Statement": [
    {
      "Sid": "Access-to-specific-bucket-only",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::prod-region-starport-layer-bucket/*"]
    }
  ]
}
```

Cree el punto final de CloudWatch Logs

Las tareas de Amazon ECS que utilizan el tipo de lanzamiento Fargate que utilizan una VPC sin una puerta de enlace a Internet y que también utilizan el controlador de **awslogs** registro para enviar información de registro a CloudWatch Logs requieren que cree `com.amazonaws.terminal` CloudWatch de VPC de la interfaz **region**.logs para registros. Para obtener más información, consulte [Uso de CloudWatch registros con puntos de enlace de VPC de interfaz](#) en la Guía del usuario de Amazon CloudWatch Logs.

Creación de una política de punto de enlace para sus puntos de enlace de la VPC de Amazon ECR

Una política de punto de conexión de VPC es una política de recursos de IAM que puede asociar a un punto de conexión cuando crea o modifica el punto de conexión. Si no adjuntas una política al crear un punto de conexión, AWS adjunta una política predeterminada que te permita el acceso total al servicio. Una política de punto de conexión no anula ni sustituye a las políticas de usuario de ni las políticas específicas de los servicios. Se trata de una política independiente para controlar el acceso desde el punto de conexión al servicio especificado. Las políticas de punto de conexión deben escribirse en formato JSON. Para obtener más información, consulte [Controlar el acceso a servicios con puntos de conexión de VPC](#) en la Guía del usuario de Amazon VPC.

Recomendamos crear una única política de recursos de IAM y adjuntarla a ambos puntos de enlace de la VPC de Amazon ECR.

A continuación, se muestra un ejemplo de una política de punto de enlace para la Amazon ECR. Esta política permite a un rol de IAM específico extraer imágenes de Amazon ECR.

```
{
  "Statement": [{
    "Sid": "AllowPull",
    "Principal": {
      "AWS": "arn:aws:iam::1234567890:role/role_name"
    },
    "Action": [
      "ecr:BatchGetImage",
      "ecr:GetDownloadUrlForLayer",
      "ecr:GetAuthorizationToken"
    ],
    "Effect": "Allow",
    "Resource": "*"
  }]
}
```

El siguiente ejemplo de política de punto de conexión impide que se elimine un repositorio especificado.

```
{
  "Statement": [{
    "Sid": "AllowAll",
    "Principal": "*",
```

```

    "Action": "*",
    "Effect": "Allow",
    "Resource": "*"
  },
  {
    "Sid": "PreventDelete",
    "Principal": "*",
    "Action": "ecr:DeleteRepository",
    "Effect": "Deny",
    "Resource": "arn:aws:ecr:region:1234567890:repository/repository_name"
  }
]
}

```

El siguiente ejemplo de política de punto de conexión combina los dos ejemplos anteriores en una única política.

```

{
  "Statement": [{
    "Sid": "AllowAll",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "*",
    "Resource": "*"
  },
  {
    "Sid": "PreventDelete",
    "Effect": "Deny",
    "Principal": "*",
    "Action": "ecr:DeleteRepository",
    "Resource": "arn:aws:ecr:region:1234567890:repository/repository_name"
  },
  {
    "Sid": "AllowPull",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::1234567890:role/role_name"
    },
    "Action": [
      "ecr:BatchGetImage",
      "ecr:GetDownloadUrlForLayer",
      "ecr:GetAuthorizationToken"
    ]
  }
],
}

```

```
"Resource": "*"
}
]
}
```

Modificación de la política de punto de enlace de la VPC para Amazon ECR

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Puntos de conexión.
3. Si aún no ha creado los puntos de enlace de la VPC para Amazon ECR, consulte [Creación de puntos de enlace de la VPC para Amazon ECR](#).
4. Seleccione el punto de enlace de la VPC de Amazon ECR al que desea agregar una política y elija la pestaña Policy (Política) en la mitad inferior de la pantalla.
5. Elija Editar política y realice los cambios en la política.
6. Elija Guardar para guardar el cambio.

Subredes compartidas

No puede crear, describir, modificar ni eliminar puntos de conexión de VPC en subredes que se compartan con usted. No obstante, puede usar los puntos de conexión de VPC en las subredes que se compartan con usted.

Prevención de la sustitución confusa entre servicios

El problema de la sustitución confusa es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En AWS, la suplantación de identidad entre servicios puede provocar un confuso problema de diputado. La suplantación entre servicios puede producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio que lleva a cabo las llamadas se puede manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente de una manera en la que no debe tener permiso para acceder. Para evitarlo, AWS proporciona herramientas que lo ayudan a proteger sus datos para todos los servicios con entidades principales de servicio a las que se les ha dado acceso a los recursos de su cuenta.

Se recomienda utilizar las claves de contexto de condición global [aws:SourceArn](#) o [aws:SourceAccount](#) en las políticas de recursos para limitar los permisos que Amazon ECR concede a otro servicio para el recurso. Utilice `aws:SourceArn` si desea que solo se asocie un

recurso al acceso entre servicios. Utilice `aws:SourceAccount` si quiere permitir que cualquier recurso de esa cuenta se asocie al uso entre servicios.

La forma más eficaz de protegerse contra el problema de la sustitución confusa es utilizar la clave de contexto de condición global de `aws:SourceArn` con el ARN completo del recurso. Si no conoce el ARN completo del recurso o si está especificando varios recursos, utilice la clave de condición de contexto global `aws:SourceArn` con caracteres comodines (*) para las partes desconocidas del ARN. Por ejemplo, `arn:aws:servicename:region:123456789012:*`.

Si el valor de `aws:SourceArn` no contiene el ID de cuenta, como un ARN de bucket de Amazon S3, debe utilizar ambas claves de contexto de condición global para limitar los permisos.

El valor `aws:SourceArn` debe ser `ResourceDescription`.

El siguiente ejemplo muestra cómo puede utilizar las claves de contexto de condición `aws:SourceAccount` global `aws:SourceArn` y las claves de contexto de una política de repositorio de Amazon ECR para permitir el AWS CodeBuild acceso a las acciones de la API de Amazon ECR necesarias para la integración con ese servicio y, al mismo tiempo, evitar el confuso problema de los diputados.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"CodeBuildAccess",
      "Effect":"Allow",
      "Principal":{
        "Service":"codebuild.amazonaws.com"
      },
      "Action":[
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Condition":{
        "ArnLike":{
          "aws:SourceArn":"arn:aws:codebuild:region:123456789012:project/project-  
name"
        },
        "StringEquals":{
          "aws:SourceAccount":"123456789012"
        }
      }
    }
  ]
}
```

```
}  
  ]  
}
```

Monitoreo de Amazon ECR

Puede supervisar el uso de la API de Amazon ECR con Amazon CloudWatch, que recopila y procesa datos sin procesar de Amazon ECR para convertirlos en métricas legibles y prácticamente en tiempo real. Estas estadísticas se registran durante un período de dos semanas para que pueda acceder a la información histórica y obtener una perspectiva sobre el uso de la API. Los datos métricos de Amazon ECR se envían automáticamente CloudWatch en períodos de un minuto. Para obtener más información al respecto CloudWatch, consulta la [Guía del CloudWatch usuario de Amazon](#).

Amazon ECR proporciona métricas basadas en el uso de la API para acciones de autorización, inserción de imágenes y extracción de imágenes.

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Amazon ECR y sus AWS soluciones. Le recomendamos que recopile datos de monitoreo de los recursos que componen su AWS solución para poder depurar más fácilmente un error multipunto en caso de que se produzca. No obstante, antes de comenzar a monitorear Amazon ECR, debe crear un plan que incluya respuestas a las siguientes preguntas:

- ¿Cuáles son los objetivos de la supervisión?
- ¿Qué recursos va a supervisar?
- ¿Con qué frecuencia va a supervisar estos recursos?
- ¿Qué herramientas de monitoreo va a utilizar?
- ¿Quién se encargará de realizar las tareas de monitoreo?
- ¿Quién debería recibir una notificación cuando surjan problemas?

El siguiente paso consiste en establecer un punto de referencia del rendimiento normal de Amazon ECR en su entorno. Para ello, se debe medir el rendimiento en distintos momentos y bajo distintas condiciones de carga. A medida que monitoree Amazon ECR, guarde los datos de monitoreo históricos para que pueda compararlos con los datos de rendimiento actual, identificar los patrones de rendimiento normal y las anomalías en el rendimiento, así como desarrollar métodos para la resolución de problemas.

Temas

- [Visualización de Service Quotas y configuración de alarmas](#)
- [Métricas de uso de Amazon ECR](#)

- [Informes de uso de Amazon ECR](#)
- [Métricas de repositorios de Amazon ECR](#)
- [Eventos de Amazon ECR y EventBridge](#)
- [Registrar las acciones de Amazon ECR con AWS CloudTrail](#)

Visualización de Service Quotas y configuración de alarmas

Puedes usar la CloudWatch consola para visualizar tus cuotas de servicio y comparar tu uso actual con las cuotas de servicio. También puede configurar alarmas para recibir notificaciones cuando se acerque a una cuota.

Para visualizar una cuota de servicio y, opcionalmente, configurar una alarma

1. Abre la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, seleccione Métricas.
3. En la pestaña All metrics (Todas las métricas), elija Usage (Uso) y, a continuación, By AWS Resource (Por recurso de AWS).

Aparecerá la lista de métricas de uso de cuotas de servicio.

4. Active la casilla situada junto a una de las métricas.

El gráfico muestra el uso actual de ese AWS recurso.

5. Para añadir su cuota de servicio al gráfico, haga lo siguiente:
 - a. Elija la pestaña Métricas diagramadas.
 - b. Elija Math expression (Expresión matemática) y Start with an empty expression (Comenzar con una expresión vacía). A continuación, en la nueva fila, en Details (Detalles), escriba **SERVICE_QUOTA(m1)**.

Se añade una nueva línea al gráfico, mostrando la cuota de servicio del recurso representado en la métrica.

6. Para ver su uso actual como porcentaje de la cuota, añada una nueva expresión o cambie la expresión SERVICE_QUOTA actual. En el caso de la nueva expresión, use **m1/60/SERVICE_QUOTA(m1)*100**
7. (Opcional) Para configurar una alarma que le notifique si se acerca a la cuota de servicio, haga lo siguiente:

- a. En la fila **m1/60/SERVICE_QUOTA(m1)*100**, en Actions (Acciones), elija el icono de alarma. Se parece a una campana.

Aparecerá la página de creación de alarmas.

- b. En Conditions (Condiciones), asegúrese de que Threshold type (Tipo de umbral) es Static (Estático) y Whenever Expression1 is (Siempre que Expression1 sea) se establece en Greater (Mayor). En than (que), escriba **80**. Esto crea una alarma que pasa al estado ALARM cuando su uso supera el 80 % de la cuota.
- c. Elija Siguiente.
- d. En la página siguiente, seleccione un tema de Amazon SNS o cree uno. Este tema se notifica cuando la alarma pasa al estado ALARM. A continuación, elija Next.
- e. En la página siguiente, escriba un nombre y una descripción para la alarma y, a continuación, elija Next (Siguiente).
- f. Elija Crear alarma.

Métricas de uso de Amazon ECR

Puedes usar las métricas CloudWatch de uso para proporcionar visibilidad sobre el uso de los recursos de tu cuenta. Usa estas métricas para visualizar tu uso actual del servicio en CloudWatch gráficos y paneles.

Las métricas de uso de Amazon ECR corresponden a las cuotas AWS de servicio. Puede configurar alarmas que le avisen cuando su uso se acerque a una Service Quota. Para obtener más información acerca de las cuotas de servicio de Amazon ECR, consulte [Cuotas de servicio de Amazon ECR](#).

Amazon ECR publica las siguientes métricas en el espacio de nombres AWS/Usage.

Métrica	Descripción
CallCount	Número de llamadas de acciones de la API realizadas desde la cuenta. Los recursos se definen por las dimensiones asociadas a la métrica.

Métrica	Descripción
	La estadística más útil de esta métrica es SUM, que represent a la suma de los valores de todas las contribuciones durante el período definido.

Las siguientes dimensiones se utilizan para ajustar las métricas de uso que publica Amazon ECR.

Dimensión	Descripción
Service	El nombre del AWS servicio que contiene el recurso. En el caso de las métricas de uso de Amazon ECR, el valor de esta dimensión es ECR.
Type	El tipo de entidad que se registra. Actualmente, el único valor válido para las métricas de uso de Amazon ECR es API.
Resource	<p>El tipo de recurso que se está ejecutando. Actualmente, Amazon ECR devuelve información sobre el uso de la API en relación con las siguientes acciones.</p> <ul style="list-style-type: none">• GetAuthorizationToken• BatchCheckLayerAvailability• InitiateLayerUpload• UploadLayerPart• CompleteLayerUpload• PutImage• BatchGetImage• GetDownloadUrlForLayer
Class	La clase de recurso a la que se realiza el seguimiento. En la actualidad, Amazon ECR no utiliza la dimensión de clase.

Informes de uso de Amazon ECR

AWS proporciona una herramienta de informes gratuita llamada Cost Explorer que le permite analizar el costo y el uso de los recursos de Amazon ECR.

Utilice Cost Explorer para ver gráficos sobre el uso y los costos. Puede ver los datos de los 13 meses anteriores y predecir la cantidad que probablemente va a gastar durante los tres meses siguientes. Puede utilizar el Cost Explorer para ver sus patrones de gasto en recursos de AWS a lo largo del tiempo, identificar aspectos que deben estudiarse más a fondo y consultar tendencias que le pueden ayudar a comprender los costos. También puede especificar intervalos de tiempo en los datos y ver los datos temporales por día o por mes.

Los datos de medición de los informes de uso y costes muestran el uso en todos los repositorios de Amazon ECR. Para obtener más información, consulte [Etiquetado de los recursos para facturación](#).

Para obtener más información sobre la creación de un informe de AWS costos y uso, consulte el [informe de AWS costos y uso](#) en la Guía del AWS Billing usuario.

Métricas de repositorios de Amazon ECR

Amazon ECR envía las métricas del recuento de extracciones del repositorio a Amazon CloudWatch. Los datos métricos de Amazon ECR se envían automáticamente CloudWatch en períodos de 1 minuto. Para obtener más información al respecto CloudWatch, consulta la [Guía del CloudWatch usuario de Amazon](#).

Temas

- [Habilitar CloudWatch las métricas](#)
- [Métricas y dimensiones disponibles](#)
- [Visualización de las métricas de Amazon ECR mediante la consola CloudWatch](#)

Habilitar CloudWatch las métricas

Amazon ECR envía métricas de repositorio automáticamente para todos los repositorios. No es necesario tomar medidas de forma manual.

Métricas y dimensiones disponibles

En las siguientes secciones se enumeran las métricas y dimensiones que Amazon ECR envía a Amazon CloudWatch.

Métricas de Amazon ECR

Amazon ECR proporciona métricas para que usted pueda monitorear sus repositorios. Puede medir el recuento de extracciones.

El espacio de nombres de AWS/ECR incluye las siguientes métricas.

`RepositoryPullCount`

El número total de extracciones de las imágenes en el repositorio.

Dimensiones válidas: `RepositoryName`.

Estadísticas válidas: Average, Minimum, Maximum, Sum, Sample Count. La estadística más útil es Suma.

Unidad: entero.

Dimensiones para las métricas de Amazon ECR

Las métricas de Amazon ECR utilizan el espacio de nombres AWS/ECR y proporcionan métricas para las dimensiones siguientes.

`RepositoryName`

Esta dimensión filtra los datos solicitados de todas las imágenes del contenedor en un repositorio específico.

Visualización de las métricas de Amazon ECR mediante la consola CloudWatch

Puede ver las métricas del repositorio de Amazon ECR en la CloudWatch consola. La CloudWatch consola proporciona una visualización detallada y personalizable de sus recursos. Para obtener más información, consulta la [Guía del CloudWatch usuario de Amazon](#).

Para ver las métricas en la CloudWatch consola

1. Abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación izquierdo, elija Metrics (Métricas) y, a continuación, All metrics (Todas las métricas).
3. En la pestaña Browse (Navegar), dentro de AWS Namespaces (Espacio de nombres), elija ECR.
4. Seleccione las métricas que desea ver. Las métricas del repositorio se clasifican como ECR > Repository Metrics (Métricas de repositorio).

Eventos de Amazon ECR y EventBridge

Amazon EventBridge le permite automatizar sus AWS servicios y responder automáticamente a los eventos del sistema, como problemas de disponibilidad de las aplicaciones o cambios de recursos. Los eventos de AWS los servicios se entregan EventBridge prácticamente en tiempo real. Puede crear reglas sencillas para indicar qué eventos le resultan de interés e incluir las acciones automatizadas que deben realizarse cuando un evento cumpla una de las reglas. Entre las acciones que se pueden activar automáticamente se incluyen las siguientes:

- Añadir eventos a grupos de CloudWatch registros en Logs
- Invocar una función AWS Lambda
- Invocar Ejecutar comando de Amazon EC2
- Desviar el evento a Amazon Kinesis Data Streams
- Activar una máquina de AWS Step Functions estados
- Notificar un tema de Amazon SNS o una cola de Amazon SQS

Para obtener más información, consulta [Cómo empezar con Amazon EventBridge](#) en la Guía del EventBridge usuario de Amazon.

Eventos de ejemplo de Amazon ECR

Los siguientes ejemplos corresponden a eventos de Amazon ECR. Los eventos se emiten en la medida de lo posible.

Evento para una inserción de imagen completada

El siguiente evento se envía cuando se completa cada inserción de imagen. Para obtener más información, consulte [Enviar una imagen de Docker a un repositorio privado de Amazon ECR](#).

```
{
  "version": "0",
  "id": "13cde686-328b-6117-af20-0e5566167482",
  "detail-type": "ECR Image Action",
  "source": "aws.ecr",
  "account": "123456789012",
  "time": "2019-11-16T01:54:34Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "result": "SUCCESS",
    "repository-name": "my-repository-name",
    "image-digest":
"sha256:7f5b2640fe6fb4f46592dfd3410c4a79dac4f89e4782432e0378abcd1234",
    "action-type": "PUSH",
    "image-tag": "latest"
  }
}
```

Evento para una acción de caché de extracción

El siguiente evento se envía cuando se intenta realizar una acción de caché de extracción. Para obtener más información, consulte [Sincronice un registro anterior con un registro privado de Amazon ECR](#).

```
{
  "version": "0",
  "id": "85fc3613-e913-7fc4-a80c-a3753e4aa9ae",
  "detail-type": "ECR Pull Through Cache Action",
  "source": "aws.ecr",
  "account": "123456789012",
  "time": "2023-02-29T02:36:48Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ecr:us-west-2:123456789012:repository/docker-hub/alpine"
  ],
  "detail": {
    "rule-version": "1",
    "sync-status": "SUCCESS",
  }
}
```

```

    "ecr-repository-prefix": "docker-hub",
    "repository-name": "docker-hub/alpine",
    "upstream-registry-url": "public.ecr.aws",
    "image-tag": "3.17.2",
    "image-digest":
      "sha256:4aa08ef415aecc80814cb42fa41b658480779d80c77ab15EXAMPLE",
  }
}

```

Evento para un escaneo de imágenes completado (escaneo básico)

Cuando el escaneo básico está habilitado para su registro, se envía el siguiente evento cuando se completa cada escaneo de imágenes. El parámetro `finding-severity-counts` solo devolverá un valor para un nivel de gravedad, si existe. Por ejemplo, si la imagen no contiene resultados de nivel CRITICAL, no se devolverá ningún recuento crítico. Para obtener más información, consulte [Escanee imágenes en busca de vulnerabilidades del sistema operativo en Amazon ECR](#).

Note

Para obtener más información sobre los eventos que Amazon Inspector emite cuando se habilita el escaneo mejorado, consulte [EventBridge eventos enviados para un escaneo mejorado en Amazon ECR](#).

```

{
  "version": "0",
  "id": "85fc3613-e913-7fc4-a80c-a3753e4aa9ae",
  "detail-type": "ECR Image Scan",
  "source": "aws.ecr",
  "account": "123456789012",
  "time": "2019-10-29T02:36:48Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ecr:us-east-1:123456789012:repository/my-repository-name"
  ],
  "detail": {
    "scan-status": "COMPLETE",
    "repository-name": "my-repository-name",
    "finding-severity-counts": {
      "CRITICAL": 10,
      "MEDIUM": 9
    }
  }
}

```

```

    },
    "image-digest":
"sha256:7f5b2640fe6fb4f46592dfd3410c4a79dac4f89e4782432e0378abcd1234",
    "image-tags": []
  }
}

```

Evento de notificación de cambio en un recurso con escaneo mejorado habilitado (escaneo mejorado)

Cuando el escaneo mejorado está habilitado para su registro, Amazon ECR envía el siguiente evento cuando se produce un cambio con un recurso que tiene habilitado el escaneo mejorado. Esto incluye la creación de nuevos repositorios, la frecuencia de escaneo de un repositorio que se está modificando o cuando se crean o eliminan imágenes en repositorios con el escaneo mejorado habilitado. Para obtener más información, consulte [Escanee imágenes en busca de vulnerabilidades de software en Amazon ECR](#).

```

{
  "version": "0",
  "id": "0c18352a-a4d4-6853-ef53-0ab8638973bf",
  "detail-type": "ECR Scan Resource Change",
  "source": "aws.ecr",
  "account": "123456789012",
  "time": "2021-10-14T20:53:46Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "action-type": "SCAN_FREQUENCY_CHANGE",
    "repositories": [{
      "repository-name": "repository-1",
      "repository-arn": "arn:aws:ecr:us-east-1:123456789012:repository/repository-1",
      "scan-frequency": "SCAN_ON_PUSH",
      "previous-scan-frequency": "MANUAL"
    },
    {
      "repository-name": "repository-2",
      "repository-arn": "arn:aws:ecr:us-east-1:123456789012:repository/repository-2",
      "scan-frequency": "CONTINUOUS_SCAN",
      "previous-scan-frequency": "SCAN_ON_PUSH"
    },
    {
      "repository-name": "repository-3",

```



```

    "repository-arn": "arn:aws:ecr:us-east-1:123456789012:repository/repository-3",
    "scan-frequency": "CONTINUOUS_SCAN",
    "previous-scan-frequency": "SCAN_ON_PUSH"
  }
],
"resource-type": "REPOSITORY",
"scan-type": "ENHANCED"
}
}

```

Evento para una eliminación de imagen

El siguiente evento se envía cuando se elimina una imagen. Para obtener más información, consulte [Eliminar una imagen en Amazon ECR](#).

```

{
  "version": "0",
  "id": "dd3b46cb-2c74-f49e-393b-28286b67279d",
  "detail-type": "ECR Image Action",
  "source": "aws.ecr",
  "account": "123456789012",
  "time": "2019-11-16T02:01:05Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "result": "SUCCESS",
    "repository-name": "my-repository-name",
    "image-digest":
"sha256:7f5b2640fe6fb4f46592dfd3410c4a79dac4f89e4782432e0378abcd1234",
    "action-type": "DELETE",
    "image-tag": "latest"
  }
}


```

Registrar las acciones de Amazon ECR con AWS CloudTrail

Amazon ECR está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Amazon ECR. CloudTrail captura las siguientes acciones de Amazon ECR como eventos:

- Todas las llamadas a la API, incluidas las llamadas desde la consola de Amazon ECR

- Todas las acciones realizadas debido a la configuración de cifrado en sus repositorios
- Todas las acciones realizadas debido a las reglas de la directiva del ciclo de vida, incluidas las acciones correctas y las que no tienen éxito

 Important

Debido a las limitaciones de tamaño de los CloudTrail eventos individuales, para las acciones de política de ciclo de vida en las que 10 o más imágenes han caducado, Amazon ECR envía varios eventos a CloudTrail. Además, Amazon ECR incluye un máximo de 100 etiquetas por imagen.

Cuando se crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Amazon ECR. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con esta información, se puede determinar la solicitud que se envió a Amazon ECR, la dirección IP de origen, quién realizó la solicitud, cuándo la realizó, así como detalles adicionales.

Para obtener más información, consulte la [Guía del usuario de AWS CloudTrail](#).

Información de Amazon ECR en CloudTrail

CloudTrail está habilitada en su AWS cuenta al crear la cuenta. Cuando se produce una actividad en Amazon ECR, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los eventos recientes en su AWS cuenta. Para obtener más información, consulte [Visualización de eventos con el historial de CloudTrail eventos](#).

Para obtener un registro continuo de los eventos de su AWS cuenta, incluidos los eventos de Amazon ECR, cree un registro. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. Al crear un registro de seguimiento en la consola, puede aplicarlo a una sola región o a todas las regiones. La ruta registra los eventos en la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para obtener más información, consulte:

- [Crear una ruta para tu AWS cuenta](#)
- [AWS integraciones de servicios con registros CloudTrail](#)

- [Configuración de las notificaciones de Amazon SNS para CloudTrail](#)
- [Recibir archivos de CloudTrail registro de varias regiones](#) y [recibir archivos de CloudTrail registro de varias cuentas](#)

Todas las acciones de la API ECR de Amazon se registran CloudTrail y se documentan en la [referencia de la API de Amazon Elastic Container Registry](#). Al realizar tareas comunes, se generan secciones en los archivos de CloudTrail registro para cada acción de la API que forma parte de esa tarea. Por ejemplo, cuando se crea un repositorio `CreateRepository` y `GetAuthorizationToken` se generan `SetRepositoryPolicy` secciones en los archivos de CloudTrail registro. Cuando inserta una imagen en un repositorio, se generan las secciones `InitiateLayerUpload`, `UploadLayerPart`, `CompleteLayerUpload` y `PutImage`. Cuando extrae una imagen, se generan las secciones `GetDownloadUrlForLayer` y `BatchGetImage`. Si desea ver ejemplos de estas tareas comunes, consulte [CloudTrail ejemplos de entradas de registro](#).

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- si la solicitud se realizó con las credenciales del nodo raíz o del usuario
- si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado
- Si la solicitud la realizó otro AWS servicio

Para obtener más información, consulte el [CloudTrailuserIdentityElemento](#).

Descripción de las entradas de archivos de registros de Amazon ECR

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud y otra información. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

CloudTrail ejemplos de entradas de registro

Los siguientes son ejemplos de entradas de CloudTrail registro para algunas tareas comunes de Amazon ECR.

Note

Estos ejemplos se han manipulado para mejorar la legibilidad. En un archivo de CloudTrail registro, todas las entradas y eventos se concatenan en una sola línea. Además, este ejemplo se ha limitado a una única entrada de Amazon ECR. En un archivo de CloudTrail registro real, puede ver las entradas y los eventos de varios servicios. AWS

Temas

- [Ejemplo: Acción de creación de repositorio](#)
- [Ejemplo: acción AWS KMS CreateGrant de la API al crear un repositorio de Amazon ECR](#)
- [Ejemplo: Acción de inserción de imágenes](#)
- [Ejemplo: Acción de extracción de imágenes](#)
- [Ejemplo: Acción de política de ciclo de vida de imágenes](#)

Ejemplo: Acción de creación de repositorio

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la CreateRepository acción.

```
{
  "eventVersion": "1.04",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:account_name",
    "arn": "arn:aws:sts::123456789012:user/Mary_Major",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-07-11T21:54:07Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      }
    }
  }
}
```

```

    }
  },
  "eventTime": "2018-07-11T22:17:43Z",
  "eventSource": "ecr.amazonaws.com",
  "eventName": "CreateRepository",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "203.0.113.12",
  "userAgent": "console.amazonaws.com",
  "requestParameters": {
    "repositoryName": "testrepo"
  },
  "responseElements": {
    "repository": {
      "repositoryArn": "arn:aws:ecr:us-east-2:123456789012:repository/testrepo",
      "repositoryName": "testrepo",
      "repositoryUri": "123456789012.dkr.ecr.us-east-2.amazonaws.com/testrepo",
      "createdAt": "Jul 11, 2018 10:17:44 PM",
      "registryId": "123456789012"
    }
  },
  "requestID": "cb8c167e-EXAMPLE",
  "eventID": "e3c6f4ce-EXAMPLE",
  "resources": [
    {
      "ARN": "arn:aws:ecr:us-east-2:123456789012:repository/testrepo",
      "accountId": "123456789012"
    }
  ],
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}

```

Ejemplo: acción AWS KMS CreateGrant de la API al crear un repositorio de Amazon ECR

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la AWS KMS CreateGrant acción que se debe realizar al crear un repositorio de Amazon ECR con el cifrado KMS activado. Por cada repositorio que se cree con el cifrado KMS activado, debería ver dos entradas de CreateGrant registro. CloudTrail

```

{
  "eventVersion": "1.05",
  "userIdentity": {

```

```

    "type": "IAMUser",
    "principalId": "AIDAIEP6W46J43IG7LXAQ",
    "arn": "arn:aws:iam::123456789012:user/Mary_Major",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Mary_Major",
    "sessionContext": {
      "sessionIssuer": {

      },
      "webIdFederationData": {

      },
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-06-10T19:22:10Z"
      }
    },
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2020-06-10T19:22:10Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "CreateGrant",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.12",
  "userAgent": "console.amazonaws.com",
  "requestParameters": {
    "keyId": "4b55e5bf-39c8-41ad-b589-18464af7758a",
    "granteePrincipal": "ecr.us-west-2.amazonaws.com",
    "operations": [
      "GenerateDataKey",
      "Decrypt"
    ],
    "retiringPrincipal": "ecr.us-west-2.amazonaws.com",
    "constraints": {
      "encryptionContextSubset": {
        "aws:ecr:arn": "arn:aws:ecr:us-west-2:123456789012:repository/testrepo"
      }
    }
  },
  "responseElements": {
    "grantId": "3636af9adfee1accb67b83941087dcd45e7fadc4e74ff0103bb338422b5055f3"
  },
  "requestID": "047b7dea-b56b-4013-87e9-a089f0f6602b",

```

```

"eventID": "af4c9573-c56a-4886-baca-a77526544469",
"readOnly": false,
"resources": [
  {
    "accountId": "123456789012",
    "type": "AWS::KMS::Key",
    "ARN": "arn:aws:kms:us-west-2:123456789012:key/4b55e5bf-39c8-41ad-
b589-18464af7758a"
  }
],
"eventType": "AwsApiCall",
"recipientAccountId": "123456789012"
}

```

Ejemplo: Acción de inserción de imágenes

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que muestra una inserción de imágenes en la que se utiliza la PutImage acción.

Note

Al insertar una imagen, también verás `InitiateLayerUploadUploadLayerPart`, y `CompleteLayerUpload` referencias en los CloudTrail registros.

```

{
  "eventVersion": "1.04",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:account_name",
    "arn": "arn:aws:sts::123456789012:user/Mary_Major",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Mary_Major",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-04-15T16:42:14Z"
      }
    }
  },
  "eventTime": "2019-04-15T16:45:00Z",

```

```

"eventSource": "ecr.amazonaws.com",
"eventName": "PutImage",
"awsRegion": "us-east-2",
"sourceIPAddress": "203.0.113.12",
"userAgent": "console.amazonaws.com",
"requestParameters": {
  "repositoryName": "testrepo",
  "imageTag": "latest",
  "registryId": "123456789012",
  "imageManifest": "{\n  \"schemaVersion\": 2,\n  \"mediaType\": \"application/
vnd.docker.distribution.manifest.v2+json\",\n  \"config\": {\n    \"mediaType\":
\"application/vnd.docker.container.image.v1+json\",\n    \"size\": 5543,\n
  \"digest\": \"sha256:000b9b805af1cdb60628898c9f411996301a1c13afd3dbef1d8a16ac6dbf503a
\"\n  },\n  \"layers\": [\n    {\n      \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n      \"size\": 43252507,\n
    \"digest\": \"sha256:3b37166ec61459e76e33282dda08f2a9cd698ca7e3d6bc44e6a6e7580cdeff8e
\"\n    },\n    {\n      \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n      \"size\": 846,\n      \"digest
\": \"sha256:504facff238fde83f1ca8f9f54520b4219c5b8f80be9616ddc52d31448a044bd
\"\n    },\n    {\n      \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n      \"size\": 615,\n      \"digest
\": \"sha256:ebbcacd28e101968415b0c812b2d2dc60f969e36b0b08c073bf796e12b1bb449\"\n
    },\n    {\n      \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n      \"size\": 850,\n      \"digest
\": \"sha256:c7fb3351ecad291a88b92b600037e2435c84a347683d540042086fe72c902b8a
\"\n    },\n    {\n      \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n      \"size\": 168,\n      \"digest\":
\"sha256:2e3debadcbf7e542e2aefbce1b64a358b1931fb403b3e4aeca27cb4d809d56c2\"\n    },
\n    {\n      \"mediaType\": \"application/vnd.docker.image.rootfs.diff.tar.gzip
\",\n      \"size\": 37720774,\n      \"digest\":
\"sha256:f8c9f51ad524d8ae9bf4db69cd3e720ba92373ec265f5c390ffb21bb0c277941\"\n
    },\n    {\n      \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n      \"size\": 30432107,\n
    \"digest\": \"sha256:813a50b13f61cf1f8d25f19fa96ad3aa5b552896c83e86ce413b48b091d7f01b
\"\n    },\n    {\n      \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n      \"size\": 197,\n      \"digest
\": \"sha256:7ab043301a6187ea3293d80b30ba06c7bf1a0c3cd4c43d10353b31bc0cecf7d
\"\n    },\n    {\n      \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n      \"size\": 154,\n      \"digest
\": \"sha256:67012cca8f31dc3b8ee2305e7762fee20c250513effdedb38a1c37784a5a2e71\"\n
    },\n    {\n      \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n      \"size\": 176,\n      \"digest
\": \"sha256:3bc892145603fffc9b1c97c94e2985b4cb19ca508750b15845a5d97becbd1a0e
\"\n    },\n    {\n      \"mediaType\": \"application/

```



```

vnd.docker.image.rootfs.diff.tar.gzip",\n          \size": 183,\n          \digest
\": \sha256:6f1c79518f18251d35977e7e46bfa6c6b9cf50df2a79d4194941d95c54258d18"\n
    },\n    {\n        \mediaType": \application/
vnd.docker.image.rootfs.diff.tar.gzip",\n          \size": 212,\n          \digest
\": \sha256:b7bcfbc2e2888afebede4dd1cd5eebf029bb6315feeaf0b56e425e11a50afe42"\n
    },\n    {\n        \mediaType": \application/
vnd.docker.image.rootfs.diff.tar.gzip",\n          \size": 212,\n          \digest\":
\sha256:2b220f8b0f32b7c2ed8eaafe1c802633bbd94849b9ab73926f0ba46cdae91629"\n    }
  ]\n}
},
"responseElements": {
  "image": {
    "repositoryName": "testrepo",
    "imageManifest": "{\n  \schemaVersion": 2,\n  \mediaType": \application/
vnd.docker.distribution.manifest.v2+json",\n  \config": {\n    \mediaType":
\application/vnd.docker.container.image.v1+json",\n    \size": 5543,\n
\digest": \sha256:000b9b805af1cdb60628898c9f411996301a1c13afd3dbef1d8a16ac6dbf503a
"\n  },\n  \layers": [\n    {\n      \mediaType": \application/
vnd.docker.image.rootfs.diff.tar.gzip",\n      \size": 43252507,\n
\digest": \sha256:3b37166ec61459e76e33282dda08f2a9cd698ca7e3d6bc44e6a6e7580cdeff8e
"\n    },\n    {\n      \mediaType": \application/
vnd.docker.image.rootfs.diff.tar.gzip",\n      \size": 846,\n      \digest
\": \sha256:504facff238fde83f1ca8f9f54520b4219c5b8f80be9616ddc52d31448a044bd
"\n    },\n    {\n      \mediaType": \application/
vnd.docker.image.rootfs.diff.tar.gzip",\n      \size": 615,\n      \digest
\": \sha256:ebbcacd28e101968415b0c812b2d2dc60f969e36b0b08c073bf796e12b1bb449"\n
    },\n    {\n      \mediaType": \application/
vnd.docker.image.rootfs.diff.tar.gzip",\n      \size": 850,\n      \digest
\": \sha256:c7fb3351ecad291a88b92b600037e2435c84a347683d540042086fe72c902b8a
"\n    },\n    {\n      \mediaType": \application/
vnd.docker.image.rootfs.diff.tar.gzip",\n      \size": 168,\n      \digest\":
\sha256:2e3debadcbf7e542e2aefbce1b64a358b1931fb403b3e4aeca27cb4d809d56c2"\n    },
\n    {\n      \mediaType": \application/vnd.docker.image.rootfs.diff.tar.gzip
",\n      \size": 37720774,\n      \digest":
\sha256:f8c9f51ad524d8ae9bf4db69cd3e720ba92373ec265f5c390ffb21bb0c277941"\n
    },\n    {\n      \mediaType": \application/
vnd.docker.image.rootfs.diff.tar.gzip",\n      \size": 30432107,\n
\digest": \sha256:813a50b13f61cf1f8d25f19fa96ad3aa5b552896c83e86ce413b48b091d7f01b
"\n    },\n    {\n      \mediaType": \application/
vnd.docker.image.rootfs.diff.tar.gzip",\n      \size": 197,\n      \digest
\": \sha256:7ab043301a6187ea3293d80b30ba06c7bf1a0c3cd4c43d10353b31bc0cecfe7d
"\n    },\n    {\n      \mediaType": \application/
vnd.docker.image.rootfs.diff.tar.gzip",\n      \size": 154,\n      \digest
\": \sha256:67012cca8f31dc3b8ee2305e7762fee20c250513effdedb38a1c37784a5a2e71"\n

```

```

    },\n    {\n        \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",,\n        \"size\": 176,\n        \"digest
\": \"sha256:3bc892145603fffc9b1c97c94e2985b4cb19ca508750b15845a5d97becbd1a0e
\\n    },\n    {\n        \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",,\n        \"size\": 183,\n        \"digest
\": \"sha256:6f1c79518f18251d35977e7e46bfa6c6b9cf50df2a79d4194941d95c54258d18\"\\n
    },\n    {\n        \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",,\n        \"size\": 212,\n        \"digest
\": \"sha256:b7bcfbc2e2888afebede4dd1cd5eebf029bb6315feeaf0b56e425e11a50afe42\"\\n
    },\n    {\n        \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",,\n        \"size\": 212,\n        \"digest\":
\"sha256:2b220f8b0f32b7c2ed8eaafe1c802633bbd94849b9ab73926f0ba46cdae91629\"\\n    }\\n
    ]\\n}\",
    \"registryId\": \"123456789012\",
    \"imageId\": {
        \"imageDigest\":
\"sha256:98c8b060c21d9adbb6b8c41b916e95e6307102786973ab93a41e8b86d1fc6d3e\",
        \"imageTag\": \"latest\"
    }
}
},
\"requestID\": \"cf044b7d-5f9d-11e9-9b2a-95983139cc57\",
\"eventID\": \"2bfd4ee2-2178-4a82-a27d-b12939923f0f\",
\"resources\": [{
    \"ARN\": \"arn:aws:ecr:us-east-2:123456789012:repository/testrepo\",
    \"accountId\": \"123456789012\"
}],
\"eventType\": \"AwsApiCall\",
\"recipientAccountId\": \"123456789012\"
}

```

Ejemplo: Acción de extracción de imágenes

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro en la que se muestra una extracción de imágenes que utiliza la BatchGetImage acción.

Note

Al extraer una imagen, si aún no la tienes localmente, también verás `GetDownloadUrlForLayer` referencias en los CloudTrail registros.

```
{
  "eventVersion": "1.04",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:account_name",
    "arn": "arn:aws:sts::123456789012:user/Mary_Major",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Mary_Major",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-04-15T16:42:14Z"
      }
    }
  },
  "eventTime": "2019-04-15T17:23:20Z",
  "eventSource": "ecr.amazonaws.com",
  "eventName": "BatchGetImage",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "203.0.113.12",
  "userAgent": "console.amazonaws.com",
  "requestParameters": {
    "imageIds": [{
      "imageTag": "latest"
    }],
    "acceptedMediaTypes": [
      "application/json",
      "application/vnd.oci.image.manifest.v1+json",
      "application/vnd.oci.image.index.v1+json",
      "application/vnd.docker.distribution.manifest.v2+json",
      "application/vnd.docker.distribution.manifest.list.v2+json",
      "application/vnd.docker.distribution.manifest.v1+prettyjws"
    ],
    "repositoryName": "testrepo",
    "registryId": "123456789012"
  },
  "responseElements": null,
  "requestID": "2a1b97ee-5fa3-11e9-a8cd-cd2391aeda93",
  "eventID": "c84f5880-c2f9-4585-9757-28fa5c1065df",
  "resources": [{
    "ARN": "arn:aws:ecr:us-east-2:123456789012:repository/testrepo",
    "accountId": "123456789012"
  }]
```

```
  ]],  
  "eventType": "AwsApiCall",  
  "recipientAccountId": "123456789012"  
}
```

Ejemplo: Acción de política de ciclo de vida de imágenes

El siguiente ejemplo muestra una entrada de CloudTrail registro que muestra cuándo una imagen ha caducado debido a una regla de política de ciclo de vida. Este tipo de evento se puede encontrar filtrando por `PolicyExecutionEvent` en el campo de nombre del evento.

Important

Debido a las limitaciones de tamaño de los CloudTrail eventos individuales, para las acciones de política de ciclo de vida en las que 10 o más imágenes han caducado, Amazon ECR envía varios eventos a CloudTrail. Además, Amazon ECR incluye un máximo de 100 etiquetas por imagen.

```
{  
  "eventVersion": "1.05",  
  "userIdentity": {  
    "accountId": "123456789012",  
    "invokedBy": "AWS Internal"  
  },  
  "eventTime": "2020-03-12T20:22:12Z",  
  "eventSource": "ecr.amazonaws.com",  
  "eventName": "PolicyExecutionEvent",  
  "awsRegion": "us-west-2",  
  "sourceIPAddress": "AWS Internal",  
  "userAgent": "AWS Internal",  
  "requestParameters": null,  
  "responseElements": null,  
  "eventID": "9354dd7f-9aac-4e9d-956d-12561a4923aa",  
  "readOnly": true,  
  "resources": [  
    {  
      "ARN": "arn:aws:ecr:us-west-2:123456789012:repository/testrepo",  
      "accountId": "123456789012",  
      "type": "AWS::ECR::Repository"  
    }  
  ],  
}
```

```

"eventType": "AwsServiceEvent",
"recipientAccountId": "123456789012",
"serviceEventDetails": {
  "repositoryName": "testrepo",
  "lifecycleEventPolicy": {
    "lifecycleEventRules": [
      {
        "rulePriority": 1,
        "description": "remove all images > 2",
        "lifecycleEventSelection": {
          "tagStatus": "Any",
          "tagPrefixList": [],
          "countType": "Image count more than",
          "countNumber": 2
        },
        "action": "expire"
      }
    ],
    "lastEvaluatedAt": 0,
    "policyVersion": 1,
    "policyId": "ceb86829-58e7-9498-920c-aa042e33037b"
  },
  "lifecycleEventImageActions": [
    {
      "lifecycleEventImage": {
        "digest":
"sha256:ddba4d27a7ffc3f86dd6c2f92041af252a1f23a8e742c90e6e1297bfa1bc0c45",
        "tagStatus": "Tagged",
        "tagList": [
          "alpine"
        ],
        "pushedAt": 1584042813000
      },
      "rulePriority": 1
    },
    {
      "lifecycleEventImage": {
        "digest":
"sha256:6ab380c5a5acf71c1b6660d645d2cd79cc8ce91b38e0352cbf9561e050427baf",
        "tagStatus": "Tagged",
        "tagList": [
          "centos"
        ],
        "pushedAt": 1584042842000
      }
    }
  ]
}

```

```
    },  
    "rulePriority": 1  
  }  
]  
}  
}
```

Uso de Amazon ECR con un SDK AWS

AWS Los kits de desarrollo de software (SDK) están disponibles para muchos lenguajes de programación populares. Cada SDK proporciona una API, ejemplos de código y documentación que facilitan a los desarrolladores la creación de aplicaciones en su lenguaje preferido.

Documentación de SDK	Ejemplos de código
AWS SDK for C++	AWS SDK for C++ ejemplos de código
AWS CLI	AWS CLI ejemplos de código
AWS SDK for Go	AWS SDK for Go ejemplos de código
AWS SDK for Java	AWS SDK for Java ejemplos de código
AWS SDK for JavaScript	AWS SDK for JavaScript ejemplos de código
AWS SDK para Kotlin	AWS SDK para Kotlin ejemplos de código
AWS SDK for .NET	AWS SDK for .NET ejemplos de código
AWS SDK for PHP	AWS SDK for PHP ejemplos de código
AWS Tools for PowerShell	Herramientas para ejemplos PowerShell de código
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) ejemplos de código
AWS SDK for Ruby	AWS SDK for Ruby ejemplos de código
AWS SDK para Rust	AWS SDK para Rust ejemplos de código
AWS SDK para SAP ABAP	AWS SDK para SAP ABAP ejemplos de código
AWS SDK para Swift	AWS SDK para Swift ejemplos de código

 Ejemplo de disponibilidad

¿No encuentra lo que necesita? Solicite un ejemplo de código a través del enlace de Enviar comentarios que se encuentra al final de esta página.

Ejemplos de código para Amazon ECR con SDK AWS

Los siguientes ejemplos de código muestran cómo utilizar Amazon ECR con un kit de desarrollo de AWS software (SDK).

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las funciones de servicio individuales, es posible ver las acciones en contexto en los escenarios relacionados y en los ejemplos entre servicios.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte [Uso de Amazon ECR con un SDK AWS](#). En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Ejemplos de código

- [Acciones para Amazon ECR mediante SDK AWS](#)
 - [Úselo DescribeRepositories con un AWS SDK o CLI](#)
 - [Úselo ListImages con un AWS SDK o CLI](#)

Acciones para Amazon ECR mediante SDK AWS

Los siguientes ejemplos de código muestran cómo realizar acciones individuales de Amazon ECR con los AWS SDK. Estos extractos se denominan API Amazon ECR y son extractos de código de programas más grandes que deben ejecutarse en su contexto. Cada ejemplo incluye un enlace a GitHub, donde puede encontrar instrucciones para configurar y ejecutar el código.

Los siguientes ejemplos incluyen solo las acciones que se utilizan con mayor frecuencia. Para obtener una lista completa, consulta la referencia de la [API de Amazon Elastic Container Registry \(Amazon ECR\)](#).

Ejemplos

- [Úselo DescribeRepositories con un AWS SDK o CLI](#)
- [Úselo ListImages con un AWS SDK o CLI](#)

Úselo **DescribeRepositories** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `DescribeRepositories`.

CLI

AWS CLI

Descripción de los repositorios de imágenes en un registro

En este ejemplo, se describen los repositorios del registro predeterminado de una cuenta.

Comando:

```
aws ecr describe-repositories
```

Salida:

```
{
  "repositories": [
    {
      "registryId": "012345678910",
      "repositoryName": "ubuntu",
      "repositoryArn": "arn:aws:ecr:us-west-2:012345678910:repository/
ubuntu"
    },
    {
      "registryId": "012345678910",
      "repositoryName": "test",
      "repositoryArn": "arn:aws:ecr:us-west-2:012345678910:repository/test"
    }
  ]
}
```

- Para obtener más información sobre la API, consulte [DescribeRepositories](#) la Referencia de AWS CLI comandos.

Rust

SDK para Rust

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
async fn show_repos(client: &aws_sdk_ecr::Client) -> Result<(),
aws_sdk_ecr::Error> {
    let rsp = client.describe_repositories().send().await?;

    let repos = rsp.repositories();

    println!("Found {} repositories:", repos.len());

    for repo in repos {
        println!("  ARN: {}", repo.repository_arn().unwrap());
        println!("  Name: {}", repo.repository_name().unwrap());
    }

    Ok(())
}
```

- Para obtener más información sobre la API, consulta [DescribeRepositories](#) la referencia sobre la API de AWS SDK para Rust.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte [Uso de Amazon ECR con un SDK AWS](#). En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **ListImages** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `ListImages`.

CLI

AWS CLI

Creación de una lista de las imágenes en un repositorio

En el siguiente ejemplo de `list-images` se muestra una lista de las imágenes del repositorio `cluster-autoscaler`.

```
aws ecr list-images \
  --repository-name cluster-autoscaler
```

Salida:

```
{
  "imageIds": [
    {
      "imageDigest":
"sha256:99c6fb4377e9a420a1eb3b410a951c9f464eff3b7dbc76c65e434e39b94b6570",
      "imageTag": "v1.13.8"
    },
    {
      "imageDigest":
"sha256:99c6fb4377e9a420a1eb3b410a951c9f464eff3b7dbc76c65e434e39b94b6570",
      "imageTag": "v1.13.7"
    },
    {
      "imageDigest":
"sha256:4a1c6567c38904384ebc64e35b7eeddd8451110c299e3368d2210066487d97e5",
      "imageTag": "v1.13.6"
    }
  ]
}
```

- Para obtener más información sobre la API, consulte [ListImages](#) la Referencia de AWS CLI comandos.

Rust

SDK para Rust

Note

Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el [Repositorio de ejemplos de código de AWS](#).

```
async fn show_images(
    client: &aws_sdk_ecr::Client,
    repository: &str,
) -> Result<(), aws_sdk_ecr::Error> {
    let rsp = client
        .list_images()
        .repository_name(repository)
        .send()
```

```
        .await?;

    let images = rsp.image_ids();

    println!("found {} images", images.len());

    for image in images {
        println!(
            "image: {}:{}",
            image.image_tag().unwrap(),
            image.image_digest().unwrap()
        );
    }

    Ok(())
}
```

- Para obtener más información sobre la API, consulta [ListImages](#) la referencia sobre la API de AWS SDK para Rust.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte [Uso de Amazon ECR con un SDK AWS](#). En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Cuotas de servicio de Amazon ECR

En la tabla siguiente se proporcionan las cuotas de servicio predeterminadas de Amazon Elastic Container Registry (Amazon ECR).

Nombre	Valor predeterminado	Ajuste	Descripción
Filtros por regla en una configuración de replicación	Cada región admitida: 100	No	El número máximo de filtros por regla en una configuración de replicación.
Imágenes por repositorio	Cada región admitida: 10 000	Sí	El número máximo de imágenes por repositorio.
Partes de capa	Cada región admitida: 4200	No	El número máximo de partes de capa. Esto solo es aplicable si utiliza las acciones de la API de Amazon ECR directamente para comenzar cargas multiparte para operaciones de inserción de imágenes.
Duración de la política del ciclo de vida	Cada región admitida: 30 720	No	Número máximo de caracteres en una política de ciclo de vida.
Tamaño máximo de parte de la capa	Cada región admitida: 10	No	Tamaño máximo (MiB) de una parte de capa. Esto solo es aplicable si utiliza las acciones de la API de Amazon ECR directamente para comenzar cargas multiparte para

Nombre	Valor predeterminado	Ajuste	Descripción
			operaciones de inserción de imágenes.
Tamaño máximo de capa	Cada región admitida: 52 000	No	Tamaño máximo (MiB) de una capa.
Tamaño mínimo de parte de la capa	Cada región admitida: 5	No	Tamaño mínimo (MiB) de una parte de capa. Esto solo es aplicable si utiliza las acciones de la API de Amazon ECR directamente para comenzar cargas multiparte para operaciones de inserción de imágenes.
Reglas de caché de extracción por registro	Cada región admitida: 50	No	Número máximo de reglas de caché de extracción.
Tasa de solicitudes de BatchCheckLayerAvailability	Cada región admitida: 1000 por segundo	Sí	El número máximo de solicitudes de la API BatchCheckLayerAvailability que se pueden realizar por segundo en la región actual. Cuando se inserta una imagen en un repositorio, se comprueba cada capa de la imagen para verificar si se ha cargado antes. Si ya se ha cargado, se omite.

Nombre	Valor predeterminado	Ajuste	Descripción
Tasa de solicitudes de BatchGetImage	Cada región admitida: 2000 por segundo	Sí	El número máximo de solicitudes BatchGetImage que se pueden realizar por segundo en la región actual. Cuando se extrae una imagen, se llama una vez a la API BatchGetImage para recuperar el manifiesto de la imagen. Si solicitas un aumento de cuota para esta API, revisa también el uso de GetDownloadUriForLayer.
Tasa de solicitudes de CompleteLayerUpload	Cada región admitida: 100 por segundo	Sí	El número máximo de solicitudes CompleteLayerUpload que se pueden realizar por segundo en la región actual. Cuando se inserta una imagen, se llama una vez a la API CompleteLayerUpload por cada capa nueva de la imagen para comprobar si la carga se ha completado.
Tasa de solicitudes GetAuthorizationToken	Cada región admitida: 500 por segundo	Sí	El número máximo de solicitudes GetAuthorizationToken que se pueden realizar por segundo en la región actual.

Nombre	Valor predeterminado	Ajuste	Descripción
Tasa de solicitudes de GetDownloadUrlForLayer	Cada región admitida: 3000 por segundo	Sí	El número máximo de solicitudes GetDownloadUrlForLayer que se pueden realizar por segundo en la región actual. Cuando se extrae una imagen, se llama una vez a la API GetDownloadUrlForLayer por capa de la imagen que aún no está almacenada en caché. Si solicitas un aumento de cuota para esta API, revisa también el uso de BatchGetImage.
Tasa de solicitudes de InitiateLayerUpload	Cada región admitida: 100 por segundo	Sí	El número máximo de solicitudes de InitiateLayerUpload que se pueden realizar por segundo en la región actual. Cuando se inserta una imagen, se llama una vez a la API InitiateLayerUpload por capa de la imagen que aún no se ha cargado. La acción de la API BatchCheckLayerAvailability determina si la capa de la imagen se ha cargado o no.

Nombre	Valor predeterminado	Ajuste	Descripción
Tasa de solicitudes de PutImage	Cada región admitida: 10 por segundo	Sí	El número máximo de solicitudes de la API PutImage que se pueden realizar por segundo en la región actual. Cuando se inserta una imagen y se han cargado todas las capas nuevas de la imagen, se llama una vez a la API PutImage para crear o actualizar el manifiesto de la imagen y las etiquetas asociadas a la imagen.
Tasa de solicitudes de UploadLayerPart	Cada región admitida: 500 por segundo	Sí	El número máximo de solicitudes de UploadLayerPart que se pueden realizar por segundo en la región actual. Cuando se inserta una imagen, cada capa nueva de la imagen se carga en partes y la API UploadLayerPart se invocará una vez por cada nueva parte de la capa de imagen.
Tasa de escaneos de imágenes	Cada región admitida: 1	No	Número máximo de escaneos de imágenes por imagen cada 24 horas.

Nombre	Valor predeterminado	Ajuste	Descripción
Repositorios registrados	Cada región admitida: 10 000	<u>Sí</u>	El número máximo de repositorios que puede crear en esta cuenta en la región actual.
Reglas por política de ciclo de vida	Cada región admitida: 50	No	El número máximo de reglas en una política de ciclo de vida
Reglas por configuración de replicación	Cada región admitida: 10	No	El número máximo de reglas en una configuración de replicación.
Etiquetas por imagen	Cada región admitida: 1000	No	El número máximo de etiquetas por imagen.
Destinos únicos en todas las reglas de una configuración de replicación	Cada región admitida: 25	No	El número máximo de destinos únicos en todas las reglas de una configuración de replicación.

Administración de las cuotas de servicio de Amazon ECR en la AWS Management Console

Amazon ECR se ha integrado con Service Quotas, un servicio de AWS que permite ver y administrar las cuotas desde una ubicación central. Para obtener más información, consulte [¿Qué son las Service Quotas?](#) en la Guía del usuario de Service Quotas.

Con Service Quotas, resulta más sencillo buscar el valor de todas las cuotas de servicio de Amazon ECR.

Visualización de las cuotas de servicio de Amazon ECR (AWS Management Console)

1. Abra la consola de Service Quotas en <https://console.aws.amazon.com/servicequotas/>.

2. En el panel de navegación, elija AWS services (Servicios de AWS).
3. En la lista AWS services (Servicios de AWS), busque y seleccione Amazon Elastic Container Registry (Amazon ECR).

En la lista Service Quotas, puede ver el nombre de la Service Quota, el valor aplicado (si está disponible), la Quota predeterminada de AWS y si el valor de Quota es ajustable.

4. Para ver información adicional sobre una cuota de servicio, como, por ejemplo, la descripción, elija el nombre de cuota.

Para solicitar un aumento de cuota, consulte [Solicitud de un aumento de cuota](#) en la Guía de usuario de Service Quotas.

Creación de una alarma de CloudWatch para monitorear las métricas de uso de las API

Amazon ECR proporciona métricas de uso de CloudWatch que se corresponden con las cuotas de servicio de AWS de cada una de las API implicadas en las acciones de autenticación de registros, inserción de imágenes y extracción de imágenes. En la consola de Service Quotas, puede visualizar la utilización en gráficos y configurar alarmas que le avisen cuando este se aproxime a una cuota de servicio. Para obtener más información, consulte [Métricas de uso de Amazon ECR](#).

Siga estos pasos para crear una alarma de CloudWatch basada en una de las métricas de uso de las API de Amazon ECR.

Creación de una alarma basada en las cuotas de uso de Amazon ECR (AWS Management Console)

1. Abra la consola de Service Quotas en <https://console.aws.amazon.com/servicequotas/>.
2. En el panel de navegación, elija AWS services (Servicios de AWS).
3. En la lista AWS services (Servicios de AWS), busque y seleccione Amazon Elastic Container Registry (Amazon ECR).
4. En la lista Service quotas (Cuotas de servicio), seleccione la cuota de uso de Amazon ECR para la que desee crear una alarma.
5. En la sección Amazon CloudWatch Events alarms (Alarmas de Amazon CloudWatch Events), elija Create (Crear).
6. En Alarm threshold (Umbral de alarma), elija el porcentaje del valor de la cuota aplicada que desee establecer como valor de la alarma.

7. En Alarm name (Nombre de la alarma), escriba el nombre de la alarma y elija Create (Crear).

Solución de problemas de Amazon ECR

Este capítulo le ayuda a encontrar información de diagnóstico para Amazon ECR y proporciona los pasos de solución de problemas y mensajes de error más comunes.

Temas

- [Solución de problemas y comandos de Docker al usar Amazon ECR](#)
- [Solución de problemas de los mensajes de error de Amazon ECR](#)

Solución de problemas y comandos de Docker al usar Amazon ECR

En algunos casos, la ejecución de un comando de Docker en Amazon ECR puede generar un mensaje de error. A continuación se explican algunos de los mensajes de error más comunes y sus posibles soluciones.

Temas

- [Los registros de Docker no contienen los mensajes de error esperados](#)
- [Error «Filesystem Verification Failed» \(Fallo al verificar el sistema de archivos\) o «404: Image Not Found» \(Imagen no encontrada\) al extraer una imagen de un repositorio de Amazon ECR](#)
- [Error «Filesystem Layer Verification Failed» \(Fallo al verificar la capa del sistema de archivos\) al extraer imágenes de Amazon ECR](#)
- [Errores HTTP 403 o error «no basic auth credentials» \(no hay credenciales de autenticación básica\) al insertar contenido en un repositorio](#)

Los registros de Docker no contienen los mensajes de error esperados

Para empezar a depurar cualquier problema relacionado con Docker, empieza por activar la salida de depuración de Docker en el daemon de Docker que se ejecuta en tus instancias host. Si utiliza imágenes extraídas de Amazon ECR en instancias de contenedor de Amazon ECS, consulte [Configuración de la salida detallada del daemon de Docker en la Guía](#) para desarrolladores de Amazon Elastic Container Service.

Error «Filesystem Verification Failed» (Fallo al verificar el sistema de archivos) o «404: Image Not Found» (Imagen no encontrada) al extraer una imagen de un repositorio de Amazon ECR

Puede producirse el error `Filesystem verification failed` al ejecutar el comando `docker pull` para extraer una imagen de un repositorio de Amazon ECR con Docker 1.9 o versiones posteriores. Es posible que reciba el error `404: Image not found` cuando utilice versiones de Docker anteriores a la 1.9.

A continuación se explican los posibles motivos.

El disco local está lleno

Si el disco local en el que ejecuta el comando `docker pull` está lleno, es posible que el hash SHA-1 que se haya calculado en el archivo local sea distinto del que haya calculado Amazon ECR. Compruebe que el disco local cuenta con suficiente espacio libre para almacenar la imagen de Docker que está extrayendo. Puede eliminar imágenes antiguas y así hacer sitio para las nuevas. Ejecute el comando `docker images` para ver una lista de las imágenes de Docker descargadas localmente y sus tamaños.

El cliente no se puede conectar al repositorio remoto debido a un error de red.

Las llamadas a un repositorio de Amazon ECR requieren conexión a Internet. Verifique la configuración de red y compruebe que otras herramientas y aplicaciones sí pueden obtener acceso a recursos en Internet. Si ejecuta `docker pull` en una instancia de Amazon EC2 en una subred privada, verifique que la subred tenga una ruta a Internet. Utilice un servidor de conversión de las direcciones de red (NAT) o una gateway de NAT administrada.

Actualmente, las llamadas a un repositorio de Amazon ECR también requieren acceso de red a Amazon Simple Storage Service (Amazon S3) a través del firewall de su compañía. Si su organización utiliza software de firewall o un dispositivo NAT que permite puntos de enlace de servicio, asegúrese de que los puntos de enlace de servicio de Amazon S3 de su región actual estén permitidos.

Si está usando Docker tras un proxy HTTP, puede configurar Docker con los ajustes del proxy correspondientes. Para obtener más información, consulte la sección [HTTP proxy](#) de la documentación de Docker.

Error «Filesystem Layer Verification Failed» (Fallo al verificar la capa del sistema de archivos) al extraer imágenes de Amazon ECR

Puede que se produzca el error `image image-name not found` al usar el comando `docker pull` para extraer imágenes. Si revisa los logs de Docker, es posible que encuentre un error como el siguiente:

```
filesystem layer verification failed for digest sha256:2b96f...
```

Este error indica que no se han podido descargar una o varias capas de la imagen. A continuación se explican los posibles motivos.

Está usando una versión antigua de Docker

Este error puede ocurrir en un reducido porcentaje de casos al utilizar una versión de Docker anterior a la 1.10. Actualice Docker a la versión 1.10 o a una posterior.

El cliente ha detectado un error de red o disco

Un disco lleno o un problema de red pueden impedir la descarga de una o varias capas, tal como se ha explicado previamente en la descripción del mensaje `Filesystem verification failed`. Siga las recomendaciones anteriores para asegurarse de que el sistema de archivos no está lleno y que la red permite el acceso a Amazon S3.

Errores HTTP 403 o error «no basic auth credentials» (no hay credenciales de autenticación básica) al insertar contenido en un repositorio

Hay ocasiones en que es posible que reciba un error HTTP 403 (Forbidden) o el mensaje de error `no basic auth credentials` desde los comandos `docker push` o `docker pull`, incluso a pesar de haberse autenticado correctamente en Docker con el comando `aws ecr get-login-password`. A continuación se indican algunas causas conocidas de este problema:

Se ha autenticado en una región diferente

Las solicitudes de autenticación están vinculadas con regiones específicas y no se pueden utilizar en otras regiones. Por ejemplo, si obtiene un token de autorización de EE. UU. Oeste (Oregón), no puede utilizarlo para autenticarse en sus repositorios en EE. UU. Este (Norte de Virginia). Para resolver el problema, asegúrese de haber recuperado un token de autenticación de la misma

región en la que se encuentra el repositorio. Para obtener más información, consulte [the section called “Autenticación del registro”](#).

Se ha autenticado para enviar a un repositorio para el que no tiene permisos

No dispone de los permisos necesarios para enviar al repositorio. Para obtener más información, consulte [Políticas de repositorios privados en Amazon ECR](#).

Su token ha caducado.

El periodo predeterminado de vencimiento de los tokens de autorización obtenidos mediante la operación `GetAuthorizationToken` es de 12 horas.

Error en el gestor de credenciales `wincred`

Algunas versiones de Docker para Windows utilizan un gestor de credenciales llamado `wincred` que no gestiona correctamente el comando de inicio de sesión de Docker generado por `aws ecr get-login-password` (para obtener más información, consulte <https://github.com/docker/docker/issues/22910>). Puede ejecutar el comando de inicio de sesión de Docker generado, pero si intenta enviar o extraer imágenes, el comando falla. Este problema se puede solucionar eliminando el esquema `https://` del argumento del registro en el comando de inicio de sesión de Docker generado desde `aws ecr get-login-password`. A continuación se muestra un ejemplo de comando de inicio de sesión de Docker sin el esquema HTTPS.

```
docker login -u AWS -p <password> <aws_account_id>.dkr.ecr.<region>.amazonaws.com
```

Solución de problemas de los mensajes de error de Amazon ECR

En algunos casos, una llamada a la API que haya iniciado a través de la consola de Amazon ECR o AWS CLI sale con un mensaje de error. A continuación se explican algunos de los mensajes de error más comunes y sus posibles soluciones.

HTTP 429: demasiadas solicitudes o `ThrottlingException`

Es posible que recibas un `429: Too Many Requests` error o un `ThrottlingException` error de una o más acciones o llamadas a la API de Amazon ECR. Esto indica que está realizando repetidamente una llamada a un único punto de enlace en Amazon ECR en poco tiempo y que se están limitando sus solicitudes. La limitación controlada ocurre cuando el número de llamadas que realiza un usuario a un único punto de enlace supera una determinada cantidad en un periodo establecido.

Cada operación de API en Amazon ECR tiene un regulador de velocidad asociado. Por ejemplo, la limitación para la acción [GetAuthorizationToken](#) es de 20 transacciones por segundo (TPS), con una ráfaga máxima permitida de hasta 200 TPS. En cada región, cada cuenta recibe un bucket que puede almacenar hasta 200 créditos de `GetAuthorizationToken`. Estos créditos se reaprovisionan a la velocidad de 20 por segundo. Si su bucket tiene 200 créditos, podría realizar hasta 200 transacciones de API `GetAuthorizationToken` por segundo durante un segundo, y luego 20 transacciones por segundo de forma indefinida. Para obtener más información sobre los límites de velocidad de las API de Amazon ECR, consulte [Cuotas de servicio de Amazon ECR](#).

Para gestionar errores de limitación controlada, implemente una función de reintento con retardo exponencial en el código. Para obtener más información, consulte el [comportamiento de los reintentos](#) en la Guía de AWS referencia de herramientas y SDK. Otra opción es solicitar un aumento del límite de velocidad, lo que puede hacer mediante la consola Service Quotas. Para obtener más información, consulte [Administración de las cuotas de servicio de Amazon ECR en la AWS Management Console](#).

HTTP 403: "User [arn] is not authorized to perform [operación]"

Es posible que aparezca el siguiente error al intentar ejecutar una acción con Amazon ECR:

```
$ aws ecr get-login-password
```

```
A client error (AccessDeniedException) occurred when calling the GetAuthorizationToken operation:
```

```
User: arn:aws:iam::account-number:user/username is not authorized to perform: ecr:GetAuthorizationToken on resource: *
```

Esto indica que al usuario no se le han concedido permisos para utilizar Amazon ECR o que los permisos no están configurados correctamente. Si está realizando acciones en un repositorio de Amazon ECR, compruebe que el usuario tiene permisos de acceso a dicho repositorio. Para obtener más información sobre cómo crear y comprobar permisos para Amazon ECR, consulte [Identity and Access Management para Amazon Elastic Container Registry](#).

Error HTTP 404: «Repository Does Not Exist» (El repositorio no existe)

Si especifica un repositorio de Docker Hub que no existe actualmente, Docker Hub lo crea de forma automática. En Amazon ECR, es necesario crear explícitamente los nuevos repositorios para poder utilizarlos. Esto impide que se creen nuevos repositorios por accidente (por ejemplo, debido a errores ortográficos) y también permite asegurarse de que a cada nuevo repositorio se le asigne

explícitamente una política de acceso de seguridad adecuada. Para obtener más información sobre la creación de repositorios, consulte [Repositorios privados de Amazon ECR](#).

Error: No se puede realizar un inicio de sesión interactivo desde un dispositivo que no sea TTY

Si recibes el error `Cannot perform an interactive login from a non TTY device`, los siguientes pasos de resolución de problemas deberían ayudarle.

- Compruebe que está utilizando la AWS CLI versión 2 y que no tiene una versión conflictiva de la AWS CLI versión 1 en el sistema. Para obtener más información, consulte [Instalación o actualización de la versión de AWS CLI más reciente](#).
- Compruebe que la ha configurado AWS CLI con credenciales válidas. Para obtener más información, consulte [Instalación o actualización de la versión de AWS CLI más reciente](#).
- Compruebe que la sintaxis del AWS CLI comando es correcta.

Historial de documentos

En la siguiente tabla se describen los cambios importantes que se han realizado en la documentación desde la última versión de Amazon ECR. Actualizamos la documentación con frecuencia para dar respuesta a los comentarios que se nos envía.

Cambio	Descripción	Fecha
Se agregó la replicación entre regiones y cuentas a las regiones de China	Amazon ECR agregó soporte a la región de China para filtrar los repositorios que se replican.	15 de mayo de 2024
Se agregó GitLab un registro de contenedores para consultar las reglas de caché	Amazon ECR agregó soporte para crear reglas de caché de extracción para el registro de GitLab contenedores.	8 de mayo de 2024
Actualización de la política de ciclo de vida de Amazon ECR para añadir compatibilidad con el uso de comodines	Amazon ECR agregó compatibilidad con comodines en una política de ciclo de vida mediante el uso del parámetro <code>tagPatternList</code> en una regla de política de ciclo de vida. Para obtener más información, consulte Automatice la limpieza de imágenes mediante políticas de ciclo de vida en Amazon ECR .	18 de diciembre de 2023
Plantillas de creación de repositorios de Amazon ECR	Amazon ECR agregó compatibilidad para las plantillas de creación de repositorios. Para obtener más información, consulte Plantillas para controlar los repositorios creados durante una acción de extracción de caché .	15 de noviembre de 2023
Se agregó la caché de extracción de Amazon ECR, compatible con los registros ascendentes autenticados	Amazon ECR agregó compatibilidad para el uso de registros ascendentes que requieren autenticación para sus reglas de caché de extracción. Para obtener más información, consulte Sincronice un registro anterior con un registro privado de Amazon ECR .	15 de noviembre de 2023

Cambio	Descripción	Fecha
AWSECRPullThroughCache_ServiceRolePolicy : actualización de una política actual	Amazon ECR agregó nuevos permisos a la política <code>AWSECRPullThroughCache_ServiceRolePolicy</code> . Estos permisos permiten a Amazon ECR recuperar el contenido cifrado de un secreto de Secrets Manager. Esto es necesario cuando se utiliza una regla de caché de extracción para almacenar en caché las imágenes de un registro anterior que requiere autenticación.	15 de noviembre de 2023
Firma de imágenes de Amazon ECR	Amazon ECR y AWS Signer se agregó soporte para crear y enviar firmas de imágenes en contenedores mediante el cliente Notary. Para obtener más información, consulte Firmar una imagen almacenada en un repositorio privado de Amazon ECR .	6 de junio de 2023
Se incorporó el registro de contenedores de Kubernetes a las reglas de caché de extracción	Amazon ECR incorporó compatibilidad para crear reglas de caché de extracción para el registro de contenedores de Kubernetes. Para obtener más información, consulte Sincronice un registro anterior con un registro privado de Amazon ECR .	1 de junio de 2023
Compatibilidad con duración de análisis mejorado de Amazon ECR	Amazon Inspector ha agregado compatibilidad para establecer el tiempo durante el que se supervisan sus repositorios cuando se habilita el análisis mejorado. Para obtener más información, consulte Cambiar la duración mejorada del escaneo de imágenes en Amazon Inspector .	28 de junio de 2022
Amazon ECR envía las métricas del recuento de extracciones del repositorio a Amazon CloudWatch	Amazon ECR envía las métricas del recuento de extracciones del repositorio a Amazon CloudWatch. Para obtener más información, consulte Métricas de repositorios de Amazon ECR .	6 de enero de 2022

Cambio	Descripción	Fecha
Compatibilidad ampliada con la replicación	Amazon ECR ha agregado compatibilidad para filtrar los repositorios que se replican. Para obtener más información, consulte Replicación de imágenes privadas en Amazon ECR .	21 de septiembre de 2021
AWS políticas gestionadas para Amazon ECR	Amazon ECR ha añadido documentación sobre las políticas AWS gestionadas. Para obtener más información, consulte AWS políticas gestionadas para Amazon Elastic Container Registry .	24 de junio de 2021
Replicación entre regiones y entre cuentas	Amazon ECR ha agregado compatibilidad con objeto de configurar los parámetros de replicación para su registro privado. Para obtener más información, consulte Configuración de registro privado en Amazon ECR .	8 de diciembre de 2020
Compatibilidad con los artefactos de OCI	Amazon ECR ha agregado compatibilidad con la inserción y extracción de artefactos de Open Container Initiative (OCI). Se ha agregado un nuevo parámetro <code>artifactMediaType</code> a la respuesta de la API <code>DescribeImages</code> para indicar el tipo de artefacto. Para obtener más información, consulte Envío de un gráfico de Helm a un repositorio privado de Amazon ECR .	24 de agosto de 2020
Cifrado en reposo	Amazon ECR ha agregado compatibilidad para configurar el cifrado de sus repositorios mediante el cifrado del lado del servidor con claves administradas por el cliente almacenadas en AWS Key Management Service (AWS KMS). Para obtener más información, consulte Cifrado en reposo .	29 de julio de 2020

Cambio	Descripción	Fecha
Imágenes multiarquitectura	<p>Amazon ECR ha agregado compatibilidad con objeto de crear e insertar listas de manifiesto Docker que se utilizan para imágenes multiarquitectura.</p> <p>Para obtener más información, consulte Envío de una imagen de arquitectura múltiple a un repositorio privado de Amazon ECR.</p>	28 de abril de 2020
Métricas de uso de Amazon ECR	<p>Amazon ECR agregó métricas CloudWatch de uso que proporcionan visibilidad del uso de los recursos de su cuenta. También puede crear CloudWatch alarmas desde la consola CloudWatch y desde la consola Service Quotas para recibir alertas cuando el uso se acerque a la cuota de servicio aplicada.</p> <p>Para obtener más información, consulte Métricas de uso de Amazon ECR.</p>	28 de febrero de 2020
Actualización de las cuotas de servicio de Amazon ECR	<p>Se han actualizado las cuotas de servicio de Amazon ECR para incluir las cuotas de cada API.</p> <p>Para obtener más información, consulte Cuotas de servicio de Amazon ECR.</p>	19 de febrero de 2020
Comando <code>get-login-password</code> agregado	<p>Se ha agregado compatibilidad para <code>get-login-password</code>, que proporciona un método simple y seguro para recuperar un token de autorización.</p> <p>Para obtener más información, consulte Uso de un token de autorización.</p>	4 de febrero de 2020

Cambio	Descripción	Fecha
Escaneo de imágenes	<p>Se ha agregado compatibilidad con el escaneo de imágenes, lo que ayuda a identificar vulnerabilidades de software en las imágenes de contenedor. Amazon ECR utiliza la base de datos de vulnerabilidades y exposiciones comunes (CVE) del proyecto CoreOS Clair de código abierto y proporciona una lista de resultados de análisis.</p> <p>Para obtener más información, consulte Escanee imágenes en busca de vulnerabilidades de software en Amazon ECR.</p>	24 de octubre de 2019
Política de punto de enlace de la VPC	<p>Se ha agregado compatibilidad para configurar una política de IAM en los puntos de enlace de la VPC de la interfaz de Amazon ECR.</p> <p>Para obtener más información, consulte Creación de una política de punto de enlace para sus puntos de enlace de la VPC de Amazon ECR.</p>	26 de septiembre de 2019
Mutabilidad de etiquetas de imágenes	<p>Se ha agregado compatibilidad para configurar un repositorio que sea inmutable y evitar que las etiquetas de imagen se sobrescriban.</p> <p>Para obtener más información, consulte Evitar que las etiquetas de imagen se sobrescriban en Amazon ECR.</p>	25 de julio de 2019

Cambio	Descripción	Fecha
Puntos de conexión de VPC de interfaz (AWS PrivateLink)	<p>Se agregó soporte para configurar puntos finales de VPC de interfaz con tecnología. AWS PrivateLink Esto permite crear una conexión privada entre su VPC y Amazon ECR sin que se requiera acceder a través de Internet, a través de una instancia NAT, una conexión de VPN o AWS Direct Connect.</p> <p>Para obtener más información, consulte Puntos de enlace de VPC de la interfaz Amazon ECR (AWS PrivateLink).</p>	25 de enero de 2019
Etiquetado de recursos	<p>Amazon ECR ha agregado compatibilidad con la adición de etiquetas de metadatos a sus repositorios.</p> <p>Para obtener más información, consulte Etiquetado de un repositorio privado en Amazon ECR.</p>	18 de diciembre de 2018
Cambio de nombre de Amazon ECR	Se ha cambiado el nombre de Amazon Elastic Container Registry (anteriormente se llamaba Amazon EC2 Container Registry).	21 de noviembre de 2017
Políticas de ciclo de vida	<p>Las políticas de ciclo de vida de Amazon ECR permiten especificar la administración de ciclo de vida de las imágenes de un repositorio.</p> <p>Para obtener más información, consulte Automatice la limpieza de imágenes mediante políticas de ciclo de vida en Amazon ECR.</p>	11 de octubre de 2017
Amazon ECR admite el manifiesto de imagen de Docker 2, esquema 2	<p>Amazon ECR admite ahora el manifiesto de imagen de Docker V2, esquema 2 (que se usa con Docker, versión 1.10 y posteriores).</p> <p>Para obtener más información, consulte Compatibilidad con el formato de manifiesto de imagen de contenedor en Amazon ECR.</p>	27 de enero de 2017

Cambio	Descripción	Fecha
Disponibilidad general de Amazon ECR	Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de Docker AWS gestionado que es seguro, escalable y fiable.	21 de diciembre de 2015

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la versión original de inglés, prevalecerá la versión en inglés.